# Crowded Places Guidance

See the latest guidance for your sector. Click on your sector to begin:

NIGHT-TIME ECONOMY

CINEMAS AND THEATRES

STADIA AND ARENAS

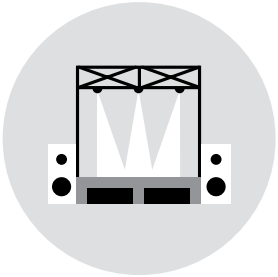
RETAIL

HEALTH

EDUCATION

PLACES OF WORSHIP

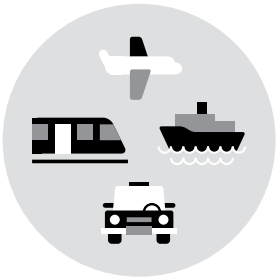
HOTELS AND RESTAURANTS



MAJOR EVENTS

VISITOR ATTRACTIONS

COMMERCIAL CENTRES



TRANSPORT

NaCTSO
National Counter Terrorism Security Office

COUNTER TERRORISM POLICING

© NaCTSO Crown copyright 2017

© Crown copyright 2017. This guidance is available under the Open Government Licence v3.0.

Disclaimer: This guidance is issued by the National Counter Terrorism Security Office NACTSO with the aim of helping organisations that provide protective security to Crowded Places to improve their protective security. It is general guidance only and needs to be adapted for use in specific situations. To the fullest extent permitted by law, NACTSO accept no liability whatsoever for any expense, liability, loss or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. You should make your own judgement as regards use of the guidance and seek independent advice as appropriate.

Version 1.00 June 2017

# Introduction

## 1. INTRODUCTION

The threat we face from terrorism is significant. As we have seen in the UK and across Europe attacks can happen at any time and any place without warning. Understanding the threat we all face and of the ways we can mitigate it can help keep us safer. Everyone can play a role in this effort by taking steps to help boost their protective security  whether that's at work, at home or away; when travelling, when out and about or just simply when online.

Having better security for all these areas makes it harder for terrorists to plan and carry out attacks. It also helps reduce the risk of other threats such as organised crime. This document provides protective security advice in a number of sectors and scenarios. It has been developed through extensive research and analysis of previous incidents, and the assessment of current known threats. It covers the key forms of protective security: physical, personnel, cyber and personal, and helps give guidance on how different sectors can act to help make their business, institutions or organisations safer.

This guidance is primarily aimed at those in the security sector and those who own or run businesses, organisations, amenities or utilities. Some of the terminology may be unfamiliar to some readers. However, we hope the advice can also be of use to anyone who wishes to improve their own security.

To deliver protective security effectively a security plan is essential along with a full risk assessment. It is important to identify an individual responsible for security and to identify what are the important assets, people, products, services, processes and information within your organisation. You can then begin to introduce mitigation to reduce vulnerabilities. A strong security culture must be supported and endorsed from a senior level.

### 1.1 Physical security

Effective physical security is best achieved by multi-layering different measures. An adversary will attempt to identify and exploit perceived weaknesses. The core principles for protecting an asset are **Deter**, **Detect**, **Delay** and initiate an effective response.

### 1.2 Personnel and people security

Personnel and people security requires the integration of physical, personnel, people and cyber security. To achieve effective personnel security a system of policies and procedures are required to reduce the risk of an organisation's assets from being exploited. This guidance will signpost you towards the objective of vigilant staff and an effective security culture. Organisations should determine how to get the best from their staff in security matters and disrupting hostile reconnaissance and insider threats.

### 1.3 Cyber security

The cyber threat as one of the most significant risks to UK interests. The National Cyber Security Centre role is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. They work together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. They are able to provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

### 1.4 Personal security

Our own security, and the safety of those close to us, is of utmost importance. The more you do to protect yourself, the safer you and your family will be. There are three key areas that can affect your safety. These are physical security, your situational awareness and online security. Exactly which security measures you adopt will depend on the extent, or level, of threat you are likely to encounter and vulnerabilities you have. This may be dependent upon your profession or role, a specific threat, the location you work and or your personal history.

No-one has more responsibility for your personal security than you. With an evolving threat we must all consider our own personal security, particularly when in crowded places.

© NaCTSO Crown copyright 2017

## LAW AND LIABILITY

There are legal and commercial reasons why venues should plan to deter terrorist and criminal acts, or at least to minimise their impact.

There is the potential of criminal prosecution and penalties under health and safety legislation for companies and individuals, particularly when statutory duties that have not been met. Where sectors are regulated it is important to liaise with the appropriate body.

**2.1 The Health and Safety at Work Act 1974 and the Management of Health & Safety at Work Regs. 1992 (updated 1999)** outlines the responsibilities of an organisation:

- The Health and Safety at Work Act 1974 and the regulations made under it, requires organisations who are duty holders to do what is reasonably practicable to ensure people's health and safety. The Act sets out the general duties that employers have towards their employees whilst at work. The Act also requires employers and the self-employed to protect people other than those at work e.g. volunteer staff and spectators. These people should be protected from risks to their health and safety arising out of, or in connection with, an employer's work activities.
- The Management of Health and Safety at Work Regulations 1999 (the Management Regulations) require organisations to assess and control risks to protect employees and others who may be effected their work activity. Where two or more employers share a workplace (whether on a temporary or a permanent basis) each employer shall have systems in place to co-operate and co-ordinate with the other employers concerned so far as is necessary to manage interfaces between activities and any shared risks.
- Co-operate and co-ordinate safety arrangements between owners, managers, security staff, tenants and others involved on site, including the sharing of incident plans and working together in testing, auditing and improving planning and response. The commercial tensions which naturally arise between landlords and tenants, and between retail tenants who may well be in direct competition with each other, must be left aside entirely when planning protective security.
- Ensure adequate training, information and equipment are provided to all staff, and especially to those involved directly on the safety and security side.
- Put proper procedures and competent staff in place to deal with imminent and serious danger and response to terrorist incidents.

**2.2 Civil Contingencies Act 2004 Part 1** places a legal obligation upon emergency services and local authorities to assess the risk of, plan, and exercise for emergencies, as well as undertake business continuity management.

Go to the Health and Safety Executive website

## 3. REPUTATION

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 protecting people against attack. Being security minded and better prepared reassures your customers and staff that you are taking security issues seriously.

**Further information**

For specific advice relating to your venue contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisers (CTSAs) through your local police force. They are co-ordinated by the National Counter Terrorism Security Office (NaCTSO).

Go to the Emergency Planning College website

Go to the Health and Safety Executive website

Go to the Occupiers' Liability Act 1957

© NaCTSO Crown copyright 2017

## CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Sectors**
Night-time economy . . . . . **6**
Cinemas and theatres . . . . . **8**
Stadia and arenas . . . . . **10**
Retail . . . . . **13**
Health . . . . . **15**
Education . . . . . **17**
Places of worship . . . . . **19**
Hotels and restaurants . . . . . **21**
Major events . . . . . **23**
Visitor attractions . . . . . **25**
Commercial centres . . . . . **27**
Transport . . . . . **29**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping . . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS) . . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction . . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour) . . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice . . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity . . . . . **150**
ETHANE . . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping . . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Night-time economy

This guide is intended to give protective security advice to those who own, operate, manage or work in the Night-Time Economy (NTE) businesses – bars, clubs and casinos. It is aimed at those places where there may be a risk of a terrorist attack by the very nature that they are crowded places. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Venues involved in the NTE differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

NTE businesses are often licensed premises and are required to make provisions to comply with the relevant legislation including the Licensing Act. Within the Act there are objectives that include the prevention of crime and disorder and the protection of public safety. Creating protective security plans to respond to terrorist type incidents will help you meet the responsibilities required within the Licensing Act and will show the extent to which your business is committed to providing a safe and secure environment.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within NTE environment. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism, for example protection from flying glass and vehicle access control measures into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, NTE venues have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your bar, club or casino could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspect items left in or around the area. In the worst case scenario your staff and guests could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your venue is to be secure, it is essential that all the work you undertake on protective security is undertaken in partnership with the police, neighbours, local and other authorities.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## NIGHT-TIME ECONOMY CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**

**Personal security**
Personal security . . . . . **127**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Cinemas and theatres

This guide is intended to give protective security advice to those who own, operate, manage or work in the cinema and theatre business. It is aimed at those places where there may be a risk of a terrorist attack by the very nature that they are crowded places. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Cinemas and theatres differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within cinemas and theatres. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism for example protection from flying glass and vehicle access control measures into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, cinemas and theatres have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your cinema or theatre could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the forms of threats or hoaxes, which are designed to frighten and intimidate. If your cinema or theatre is to be safe, it is essential that all the work you undertake on protective security is done in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## CINEMAS AND THEATRES CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**

**Personal security**
Personal security . . . . . **127**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Stadia and arenas

This guide is intended to give protective security advice to those who own, operate, manage or work in sports stadia and arenas. It is aimed at those places where there may be a risk of a terrorist attack by the very nature that they are crowded places. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Sports stadia and arenas differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

Furthermore, tragic events around the world have shown that terrorist groups have targeted sporting venues, sports teams and events in public spaces. These incidents identify that terrorists are prepared to use different methodologies to attack sites and online terrorist media seeks to incite, inspire and enable individuals and groups to target these venues. Recent events have shown that you cannot hold a safe event without considering security and, you cannot hold a secure event without considering safety.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within sports stadia and arena environments. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means and sports stadia and arenas have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your sports stadia and arenas could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your sports stadia and arenas are to be safe and secure, it is essential that all the work you undertake on protective security is done so in partnership with the police, other authorities (as appropriate) and your neighbours.

© NaCTSO Crown copyright 2017

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Wherever possible, additional security measures should be integrated with the existing security regime.

Other guidance and legislation include The Guide to Safety at Sports Grounds, the Sports Ground Safety Act 1975 and Fire Safety and Safety of Places of Sport Act 1987.

Go to the Health and Safety Executive entertainment webpage

Go to the Health and Safety Executive event safety webpage

Go to the Health and Safety Executive crowd management webpage

Go to the Health and Saftety Executive incidents and emergencies webpage

Go to the Safety at Sports Grounds website

© NaCTSO Crown copyright 2017

## STADIA AND ARENAS CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

Sector

# Retail

This guide is intended to give protective security advice to those who own, operate, manage or work in retail destinations including, shopping centres, retail parks, outlet centres, transport hubs and leisure destinations. It is aimed at those places where there may be a risk of a terrorist attack by the very nature that they are crowded places. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Shopping centres differ in many ways including size, location, layout, operation and that elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as is reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within retail environments. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism, for example protection from flying glass and vehicle access control measures into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means and retail destinations have regularly been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your retail destination could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and customers could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be achieved through the interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your retail environment is to be secure, it is essential that all the work you undertake on protective security is done so in partnership with the police, other authorities or stakeholders (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Wherever possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## RETAIL CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

Sector

# Health

This guide is intended to give protective security advice to those who are working across the health sectors and it highlights the vital part you can play in the UK counter terrorism strategy. It is likely that a healthcare provider will form part of the response to a terrorist attack, treating those injured in an incident. The health sector is also more likely to experience disruption as a secondary consequence, such as managing and responding to contamination, supporting families and managing the media. As well as working with key emergency services and stakeholders on wider civil resilience, the health sector will also be involved in ensuring business continuity management during the course of an incident.

The aim is to reduce the risk of a terrorist attack and limit the impact an attack might cause. Health sectors differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within the health sector, this guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism, for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, the health sector has previously been targeted. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your hospital or surgery for example could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff, patients and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your venue is to be safe and secure it is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## HEALTH CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Education

This guide is intended to give protective security advice to those who are responsible for the security of higher and further education institutions, irrespective of size and location. It highlights the part institutions can play in the UK counter terrorism strategy, and how by mitigating the risk you can allow teaching, learning, research, knowledge transfer, community engagement and enterprise to continue as normal. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. Higher and further education institutions differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within education environments, it is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond the risk of terrorism, for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally.

Terrorists have both the desire and intent to attack crowded places by any means, education venues have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your higher and further education institutions could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and students could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your environment is to be safe and secure it is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

Go to the Department for Education webpage

Go to the OEAP National guidance webpage

© NaCTSO Crown copyright 2017

## EDUCATION CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Places of worship

This guide is intended to give protective security advice to those who are responsible for security in places of worship. It is aimed at those places where there may be a risk of a terrorist attack either because of the nature of the place of worship or the number of people who congregate in it. The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Places of worship differ in many ways including size, location, layout, operation and that elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within places of worship. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, places of worship have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your place of worship could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and congregation could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your place of worship is to be safe and secure, it is essential that all the work you undertake on protective security is in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson (which remain the greatest threats to places of worship). Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## PLACES OF WORSHIP CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**

**Personal security**
Personal security . . . . . **127**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Hotels and restaurants

This guide provides protective security advice to those who own, operate, manage or work in hotels and restaurants. It is aimed at those places where there may be a risk of a terrorist attack by the very nature that they are a crowded place. It highlights the vital part you can play in the UK counter terrorism strategy. Hotels and restaurants differ in many ways including size, location, layout and operation and elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within hotels and restaurant environments. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism, for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, hotels and restaurants have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your hotel or restaurant could be the target of a terrorist incident. This might include having to deal with a bomb threat suspicious items left in or around the area. In the worst case scenario your staff and guests could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through the interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your hotel or restaurants is to be safe and secure it is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## HOTELS AND RESTAURANTS CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Major events

This guide is intended to give protective security advice to those who are responsible for organising major events and event security, irrespective of size and capacity and is not specific to any particular type of event. It is aimed at those events where there may be a risk of a terrorist attack either because of the nature of the event or the number or nature of the people who host or attend.
It highlights the vital part you can play in the UK counter terrorism strategy.

Furthermore, tragic events around the world have shown that terrorist groups have targeted public event spaces previously. These incidents identify that terrorists are prepared to use different methodologies to attack sites and online terrorist media seeks to incite, inspire and enable individuals and groups to target these venues. Recent events have shown that you cannot hold a safe event without considering security and, you cannot hold a secure event without considering safety.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within major events environments. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means and events have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that your event could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and event goers could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your event is to be safe and secure it is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

Go to the Health and Safety Executive entertainment webpage

Go to the Health and Safety Executive event safety webpage

Go to the Health and Safety Executive crowd management webpage

Go to the Health and Saftety Executive incidents and emergencies webpage

Go to the Health and Saftety Executive events webpage

© NaCTSO Crown copyright 2017

## MAJOR EVENTS CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Visitor attractions

This guide provides protective security advice to those who own, operate, manage or work in visitor attractions. It aids those who are seeking to reduce the risk of a terrorist attack and limit the damage an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy.

Tourism is an important and fast growing industry. It is also one of the most vulnerable, offering terrorists and organised criminals a range of high profile targets. Visitor attractions may be particularly at risk, as they are often important cultural, religious or political symbols. Visitor's enjoyment is the principal objective of the owners and managers of all attractions, this requires a secure and safe environment. We urge every attraction owner and manager to review this document and initiate such measures and preparations, procedures and training, as appropriate.

The guide seeks to reduce the risk of a terrorist attack and limit the impact an attack might cause. Visitor attractions differ in many ways including size, location, layout, operation and that some of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within visitor attraction environments, this guide is not intended to create a 'fortress mentality'.

However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond to the risk of terrorism, for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means, visitor attractions have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. In the worst case scenario your staff and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack. If your visitor attraction is to be safe and secure it is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

Go to the Health and Safety Executive entertainment webpage

Go to the Health and Safety Executive event safety webpage

Go to the Health and Safety Executive crowd management webpage

Go to the Health and Saftety Executive incidents and emergencies webpage

© NaCTSO Crown copyright 2017

## VISITOR ATTRACTIONS CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Commercial centres

This guide is intended to give protective security advice to those who are responsible for security in commercial centres. It is aimed at those places where there may be a risk of a terrorist attack either because of the nature of the building, the location or the number of people who work in it. The guide seeks to reduce the risk of a terrorist attack and limit the damage an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy. Commercial centres differ in many ways including size, location, layout, operation and elements of the advice included in this document may have already been introduced at some locations.

It is accepted that the concept of absolute security is almost impossible to achieve in combatting the threat of terrorism, but it is possible, through the use of this guidance, to reduce the risk to as low as reasonably practicable. It is recognised that there is a need to maintain a friendly and welcoming atmosphere within commercial centre  environments. This guide is not intended to create a 'fortress mentality'. However, a balance must be struck and proportionate protective security measures introduced to mitigate and respond the risk of terrorism, for example protection from flying glass and vehicle access controls into crowded areas, goods and service yards.

In recent years there has been an increase in terrorist activity both at home and abroad with the threat stemming from both international terrorism and domestic extremism. Crowded places and places of community significance are often the target of such attacks globally. Terrorists have both the desire and intent to attack crowded places by any means and commercial centres have previously been targeted throughout the world. Terrorists have the ability to both identify and exploit weaknesses in protective security. It is the aim of this guide to not only help you identify weaknesses in your protective security but also proactively work towards an improved security culture which helps to protect you and your staff from the threat of terrorism.

It is possible that commercial centres  could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area. In the worst case scenario your staff and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Methods of attack are not just physical, some attacks may be through interference with vital information or communication systems, others may be enabled by an 'insider' or by someone with specialist knowledge or access to your venue. The threat of terrorism may also take the form of threats or hoaxes, which are designed to frighten and intimidate. If your commercial centre environment is to be safe and secure it is essential that all the work you undertake on protective security is done in partnership with the police, other authorities (as appropriate) and your neighbours.

It is worth remembering that implementing measures for countering terrorism will also work against other forms of criminality, such as theft, burglary and arson. Where possible, additional security measures should be integrated with the existing security regime.

© NaCTSO Crown copyright 2017

## COMMERCIAL CENTRES CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**
Digital built assets and environments . . . . . **105**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Transport



## 1. INTRODUCTION

The Department for Transport (DfT) is responsible for and sets a counter-terrorism security policy, issues regulations and undertakes compliance activity across a number of transport modes including the aviation, maritime and rail sectors. This includes implementing International and European requirements, where they exist. DfT aims to protect the travelling public, transport facilities and those working in transport primarily from terrorist acts, and to retain public confidence in transport security in a proportionate manner.

Go to the DfT transport security webpage

### 1.1 Maritime

As an island nation, over 90% of the United Kingdom's imports and exports, by volume, arrive by sea. The maritime sector is essential to the prosperity of the UK. The maritime (including marine) sector contributes at least £13.4 billion to the UK economy and provides direct employment to at least 111,000 people. There are over 400 port facilities in the UK serving vessels engaged in a wide variety of activities.

Maritime security is governed by an international framework. In 2004, the International Maritime Organisation developed "The International Ship and Port Facility Security Code" ("the ISPS Code") which is a comprehensive set of measures to enhance the security of ships and port facilities. This has been mandated in EU law by Regulation (EC) 725/2004.

The Department for Transport, as the statutory regulator for maritime security, is responsible for ensuring that suitable and proportionate protective security measures are in place to protect ships, ports and passengers in the UK against terrorist threats. DfT has a compliance regime in place with regular inspections of ships (conducted by the Maritime and Coastguard Agency) and port facilities to ensure compliance with ISPS requirements. More information on the UK's maritime security programme, including the applicable legislation, can be found on the maritime security programme webpage.

Go to the Maritime security programme webpage

### 1.2 Aviation

The aviation sector is extremely diverse. It involves aircraft such as balloons and airships, gliders, micro-lights, helicopters, light aircraft and business jets. Their activities cover anything from agricultural use, aerial surveys, delivery of goods, corporate flights and leisure. The aerodromes that support these activities vary from individual landing strips or helipads to regional airports. This guide is intended to give protective security advice to those who work within the general aviation sector to reduce the opportunity of a terrorist attack occurring, or limit the damage such an event might cause.

Aviation is one of the most important and rapidly expanding industries within the United Kingdom. It also offers terrorists and organised criminals a range of high profile targets or a possible method of attack delivery. A successful terrorist incident on any section of the industry will have devastating consequences in terms of casualties and a loss of confidence by the travelling public.

### 1.3 Road transport

The security guidelines contained within this guidence recommend best practices, measures and procedures those managers of road transport companies, including those responsible for hiring or leasing vehicles. The objective is to raise security awareness and assist road transport companies that transport people, high consequence dangerous goods, chemicals, drugs, foodstuffs and other goods that because of their nature or value or destination may be vulnerable to terrorist, criminal acts. The carriage of dangerous goods by road is subject to international requirements, which the DfT enforces.

This guidance has been developed to help you devise and maintain a range of best practice security measures to prevent, protect and deter acts of violence including terrorism against buses, coaches, HGVs and other commercial vehicles. It covers vehicles, stations, termini and depots, and generic security advice on physical, personnel security, information and personal security.

© NaCTSO Crown copyright 2017

**1.4 Rail**

Unlike aviation and maritime and with the exception of the Channel Tunnel, the rail network within Great Britain is open i.e. there is no need to pre-book or pass through any form of security checks to use the network. However, security is taken very seriously by the DfT and it sets legal requirements and provides advice and guidance for rail operators to follow. It actively works with the industry, other Government Departments and the British Transport Police (BTP) to ensure the risks are well understood and communicated as appropriate and that mitigation measures are proportionate and practical.

The Treaty of Canterbury signed by the UK and France established the need for the defence of the Channel Fixed Link. The Channel Tunnel Act 1987 and the Channel Tunnel (Security) Order 1994 are the UK's domestic legislation that provides the legal framework to do this. In the UK, the Concessionaire and other operators of Tunnel services are responsible for the day-to-day delivery of security which includes, amongst other measures, the screening of vehicles, passengers, baggage and freight. Security in France is the responsibility of the French government, but UK and French government officials meet regularly to ensure comparability of security arrangements. The Department also meets with industry and other government agencies regularly, to review security measures.

**Primacy for security regulation is the responsibility of the Department for Transport.**

Go to the Channel Tunnel (Security) Order 1994

© NaCTSO Crown copyright 2017

## TRANSPORT CONTENTS

Click on the relevant section. At the end of each section there is a link to return to the general contents page.

**How to use this guide**

**Managing the threat**
Managing risk, business continuity . . . . . **32**
Threat level and building response plans . . . . . **40**
Communication . . . . . **42**
Suspicious items . . . . . **44**
Good housekeeping. . . . . **46**

**Attack methodology**
Improvised Explosive Devices (IEDs) . . . . . **47**
Vehicle bombs . . . . . **49**
Bomb threats . . . . . **52**
Chemical, Biological, Radiological (CBR) attacks . . . . . **56**
Firearms and weapons attack RUN, HIDE, TELL . . . . . **59**
Unmanned Aircraft Systems (UAS). . . . . **61**
Vehicle as a weapon . . . . . **66**

**Physical security**
Physical security introduction. . . . . **67**
Evacuation, invacuation, lockdown, protected spaces . . **72**
CCTV . . . . . **89**
Access control . . . . . **93**
Search planning . . . . . **96**
Mail handling . . . . . **98**
Hostile Vehicle Mitigation (HVM) . . . . . **102**

**Personnel and people security**
Personnel and people security introduction . . . . . **107**
Personnel security training and good practice . . . . . **113**
Hostile reconnaissance (suspicious behaviour). . . . . **117**
Document awareness . . . . . **120**
Guidance for commercial vehicles and hire companies **122**

**Personal security**
Personal security . . . . . **127**
Overseas travel advice. . . . . **131**

**Cyber security**
Cyber security . . . . . **135**

**Checklists**
Personnel security . . . . . **140**
CCTV . . . . . **142**
Access control . . . . . **144**
Bomb threats . . . . . **146**
Emergency and business continuity. . . . . **150**
ETHANE. . . . . **152**
Cyber security . . . . . **153**
Search planning . . . . . **154**
Crisis response kits . . . . . **156**
Good housekeeping. . . . . **159**
Suspicious behaviour reporting . . . . . **161**

© NaCTSO Crown copyright 2017

# Managing risk, business continuity

## 1. INTRODUCTION: MANAGING THE RISKS

Managing the risk of terrorism is only one part of a manager's responsibility when preparing contingency plans in response to any incident in or near their premises or event which might prejudice staff safety, public safety or disrupt normal operations. It is important that this is one person's function and responsibility. The governing body or board is ultimately responsible and must be committed to managing the risks and understand the consequences of ineffective management.

Robust risk management processes will anticipate and assess risks to the organisation. The risks should be mitigated through preventative measures such as 'target hardening', training of personnel and information security systems, Having worked on preventing the risk materialising, the organisation must still be ready to respond and recover from a business interruption, regardless of its cause. There are a number of phases in a response which are summarised in diagram 1.

### 1.1 Emergency response

This deals with immediate impacts of an incident, a relatively short term phase that focuses on ensuring people and the environment are made safe.

### 1.2 Incident Management (IM)

How the organisation will manage the consequences of the business interruption through command, control, coordination and communication. (IM covers who is in charge, how to keep stakeholders informed, escalation processes, coordination of resources, etc.)

### 1.3 Crisis management

Crisis management is about your arrangements to manage strategic, complex and unprecedented events. It is rarely standalone and will require integration with other disciplines. Note that an incident may require a crisis management response without business continuity plan activation, such as in the event of major negative media attention about the business. In contrast there may be a 'creeping crisis' where a disruption such an attack on an IT system emerges and, if not managed effectively, turns into a crisis. Therefore, the incident response arrangements must be flexible enough to manage both an operational disruption which may need to be escalated and a crisis situation which requires strategic leadership.

### 1.4 Business Continuity (BC)

These are the arrangements you should develop, to maintain critical and urgent business activities to a pre-determined level i.e. what work your business must continue to do to survive the disruption from a terrorist attack. Consider a range of impacts that could disrupt your business, including the unavailability of your building (through loss of utilities or evacuation), people (colleagues and suppliers) and equipment (machinery and IT). Then plan how you would continue critical parts of your business during disruption.

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. An attack on a crucial contractor or supplier can also impact on your 'business as usual', so will need to be included in your business continuity plan. This is particularly relevant for smaller operations that may not have the resources to withstand even a few days financial loss. Make sure you include consideration of sub-contractors to your principal contractors.

International Standards ISO 22301 Societal Business Management Security Systems and Guidance provides further informantion on the subject of business continuity plans.

Free practical advice is available from your local authority or from the Business Emergency Resilience Group, a Prince of Wales initiative.

You may also want to complete the Business continuity checklist

For advice and training on resilience contact the Emegerncy Planning College (EPC)

Go to the Business Emergency Resilience Group website

Go to the Cabinet office website

© NaCTSO Crown copyright 2017

Go to the Government Emergncies, preparation, response, recovery webpage

Go to the Government Emergency planning webpage

**1.5 Recovery**

This is a plan that usually takes place over a long duration, with wider stakeholder engagement and detailing the priorities for rebuild, recovery and restoration. How and in what order you will return to the new normality following a disruption.

Response and recovery usually overlap – there is a transitional phase. After each activation of resilience arrangements, a formal debrief should be conducted in order to continuously improve.

**Diagram 1**

## RESPONSE ACTIVITY OVER TIME

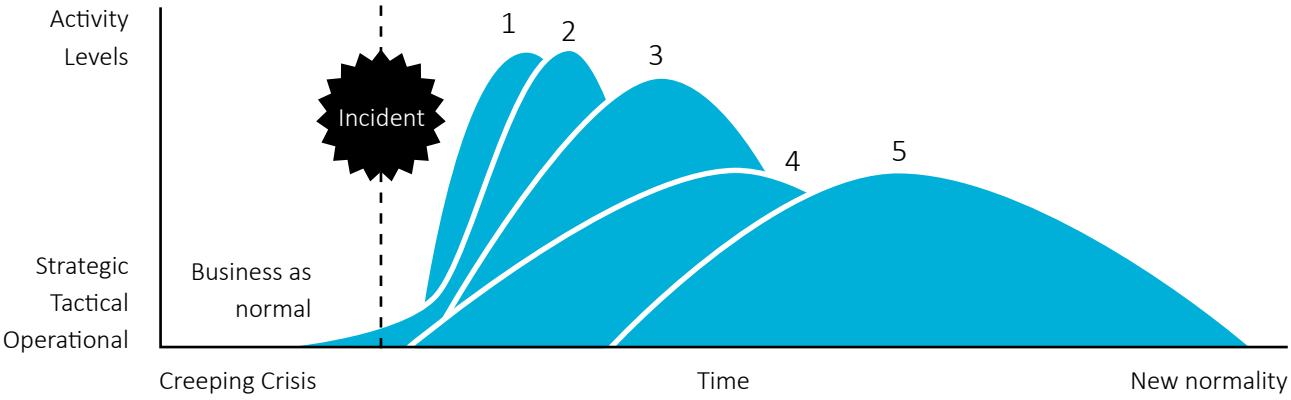
**1. Emergency Services**
Response safeguarding life, protecting environment and company assets

**2. Incident management**
Command, control, coordination, communication

**3. Crisis management**
Strategic, complex and unprecedented reputation stakeholder confidence

**4. Business continuity**
Maintaining critical activities

**5. Recovery**
Focussed on rebuilding, restoring and rehabitation




Risk management
prevention and preparation

©Emergency Planning College 2017

© NaCTSO Crown copyright 2017

## 2. REPUTATION

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

## 3. NEIGHBOURS AND PARTNERS

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.

A number of organisations have adopted good practice to enhance the protective security measures in and around their premises. This document identifies and complements such good practice.

This guide recognises that crowded places differ in many ways including, size, location, staff numbers, layout, footfall and operation and that some of the advice included in this document may have already been introduced at some locations. Consider it work you undertake on protective security that is progressed in partnership with the emergency services, other authorities as appropriate and your neighbours, if your premises are to be secure.

## 4. MANAGING THE RISK

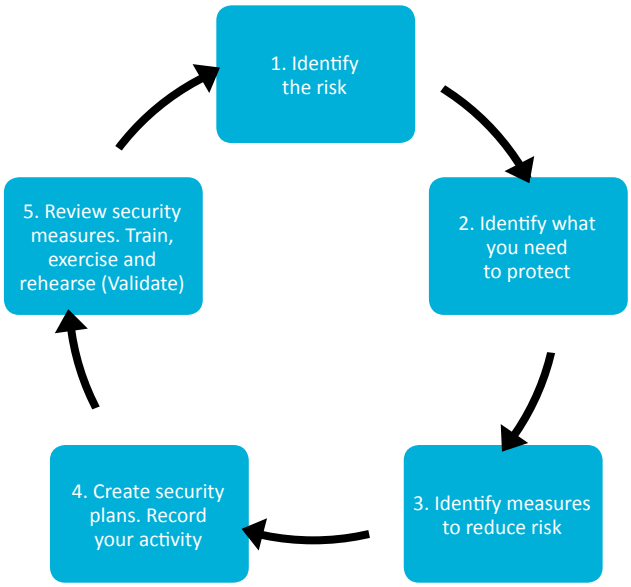
With regard to protective security, the best way to manage the hazards and risks to your business is to start by understanding and identifying the threats, vulnerabilities and the resulting business impact.

This will help you to decide:

- what protective security improvements you need to make
- what type of security and contingency plans you need to develop

For some crowded places simple good practice, coupled with staff 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.

The following diagram illustrates a typical risk management cycle:




**Step One: Identify the risk**

Understanding the terrorist's intentions and capabilities, what they might do and how they might do it, is crucial to assessing risk. This guidance outlines in other chapters the threat and some of the current terrorist attack methodologies. Ask yourself the following questions:

- What can be learnt from the government and media about the current security climate locally and globally, or about recent terrorist activities?
- See www.cpni.gov.uk or the useful contacts section at the back of this booklet.
- Is there anything about the location of your premises, its visitors, sponsors, contractors, occupiers and staff, your activities, or within the wider community that may attract a terrorist attack?
- Is there an association with high profile individuals or organisations which might be terrorist targets?

© Crown copyright 2017

- Do you have procedures in place and available for deployment on occasions when VIPs attend any events at your crowded place? How often are they reviewed? Have you resources and funding when required?
- Does your location mean you could suffer collateral damage from an attack or other incident at a 'high risk' prestigious neighbouring premises?
- What can your local police service tell you about crime and other problems in your area?
- Are there any aspects of your business or activities, or those of your staff that terrorists might wish to exploit to aid an attack; such as building floor plans, publically available documents, technical expertise or poor security culture such as unauthorised access to restricted areas?
- Do you communicate information about the threat and building response levels to your staff?
- Do you train and advise your staff to take a level of personal responsibility given the environment and threat of terrorism we face in society in general?
- Do your contracts with other companies restrict what information they can publish online about you such as information or image of your site etc.?
- Does anything identify vital installations or services to the continuation of business in your premises?

Read more about Digital built assets and environments

Go to the CPNI website

**Step Two: Decide what you need to protect and identify your vulnerabilities**

Now that you have determined the risks you can identify what you need to protect. Your priorities for protection should fall under the following categories:

- people (e.g. staff, visitors, customers, contractors, general public)
- physical assets (e.g. buildings, contents, equipment, plans and sensitive materials)
- information (e.g. electronic and paper data)
- processes and policies (e.g. supply chains, critical procedures) – the actual operational process and essential services required to support it.

For each, you need to consider:

- what is the vulnerability?
- why is it vulnerable?
- what are they vulnerable to?

You know what is important to you and 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. You should already have plans in place for dealing with fire and crime, procedures for assessing the integrity of those you employ, protection from IT viruses, and measures to secure parts of the premises.

**Step Three: Identify measures to reduce risk**

Having identified what you need to protect and why, you need to understand what measures your site has in place already, how effective they are and where the vulnerabilities are. The measures you use should be proportionate and cost effective; measures should work together to produce an integrated system.

An integrated approach to security is essential. This involves thinking about physical security, cyber security, personnel security (i.e. good recruitment and employment practices) and personal security. There is little point investing in costly security measures if they can be easily undermined by a disaffected member of staff, supplier or contractor by a poor recruitment and or procurement process. This guidance identifies and signposts to measures that you implement to assist to mitigate the risks.

Remember, TERRORISM IS A CRIME. Many of the security precautions typically used to deter criminals are also effective against terrorists. So before you invest in additional security measures, review what you already have in place. You may already have a good safety and security culture, on which you can build.

© NaCTSO Crown copyright 2017

If you need additional security measures, then make them cost-effective by careful planning wherever possible.

Introduce new equipment or procedures in conjunction with building work. In multi-occupancy buildings, try to agree communal security arrangements.

Even if organisations or businesses surrounding your location are not concerned about terrorist attacks, they will be concerned about general crime, your security measures will help protect against crime as well as terrorism.

Staff may be unaware of existing security measures, or may have developed habits to circumvent them, such as short cuts through fire exits. Simply reinstating good basic security practices and regularly reviewing them will bring benefits at negligible cost.

Go to the CPNI Operational Requirements webpage

**Step four: Create security plans**

**Security planning**

See table 1.

Following a risk assessment, it is recognised that for the majority of crowded place sites and venues the responsibility for implementation of protective security measures will fall on a security manager or an assigned individual. They must have sufficient authority to direct the action taken in response to the risk.

They must be involved in the planning of the perimeter security, access control, glazing, contingency plans etc. so that the terrorist dimension is taken into account. The security manager must similarly be consulted over any new building or renovation work, so that counter terrorism specifications, such as glazing and physical barriers can be factored in.

The security manager at most crowded places should already have responsibility for most if not all of the following key areas:

- The production of the security plan based on the risk assessment.
- The formulation and maintenance of a search plan.
- The formulation and maintenance of plans for dealing with for example bomb threats, suspect packages and evacuation.
- Liaising with the police, other emergency services and local authorities.
- Arranging staff training, exercises, rehearsal, testing and exercising. Include their deputies and conduct briefings and debriefings.
- Conducting regular reviews of the plans.

**Creating your security plans**

Effective security plans are those that are simple, clear and flexible. The security planner should call upon staff with particular business area knowledge to help, such as IT, Procurement or HR manager (to consider countering the insider threat for example).

Plans should be:

- **Protective** i.e. the site search plan to counter the threat of a placed Improvised Explosive Device (IED), security patrols, deployment of CCTV, staff training etc.
- **Response** i.e. the actions staff should take if they identify a person acting suspiciously, discover a suspicious item, are receipt of a bomb threats, malware, if there is a need to evacuate or invacuation, a communication and media strategy etc.

© NaCTSO Crown copyright 2017

The planning should include:

| | |
|---|---|
| **Policy** | Be clear and document what you want to achieve. |
| **Operational** | Put processes in place to make the policy work. |
| **Physical** | The "hardware" that supports any operational process. |
| **Training and awareness** | Make sure those with a role to play in the security welfare of the site are properly educated and equipped to act confidently and effectively. |
| **Validation** | Agree and implement appropriate measures to validate plans and arrangements. These may include exercises, tests or other techniques to establish the suitability, sufficiency and effectiveness of your arrangements. |
| **Partnership** | Working with those who can or are needed to make security work. |
| **Review and monitor** | Conduct regular reviews or following any change in circumstances such as a change in threat, circumstances, environment, post an incident or changes in. |
| **Communication and media** | Identify how you will communicate with staff, visitors, suppliers and contractors. |

Table 1.

**Action plans**

To help progress security planning it is good practice to create an action plan. The action plan should set out:

- the activity to be undertaken
- brief rationale for the activity
- the name of the person responsible for completing the action
- a start date, review date and realistic completion date
- a scale to measure the actions progress, i.e. red, amber or green

The action plan will form an important part of your security audit.

**Step Five: Review your security measures; train staff, rehearse, exercise and test security plans**

You should regularly review and exercise your plans to ensure that they remain accurate, workable and up to date. Additionally if there is an attack elsewhere or change in threat or circumstance including to suppliers, contractors or stakeholders consider reviewing your plans. Through training make sure that your staff understand their personal responsibilities 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. Rehearsals and exercises should wherever possible, be conducted in conjunction with all partners, emergency services and local authorities.

© NaCTSO Crown copyright 2017

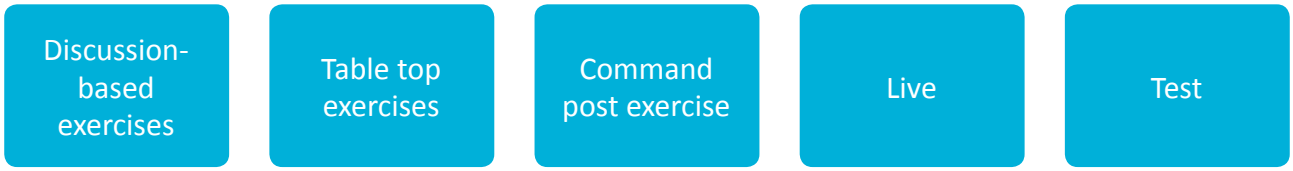
Managing risk and security planning are on-going processes. Part of the validation process is to exercise your plans and use any learning to further refine and ensure plans are workable and achieve the required outcomes.

The aim of your exercises should be to:

- ensure that plans work (verification)
- develop staff and third party competencies and enable them to practice carrying out and understanding their roles in the plan (training)
- test established procedures to ensure they remain valid (exercise, rehearse and validation)
- provide learning to further refine the plan (review)

Developing an exercise programme. The Business Continuity Institute (BCI) outlines five categories of exercising; they range in scale and complexity.

Main levels of exercise are:




**BCI Good Practice Guidelines Training Course Module Six Version 1.0**

| **Plan Review (Discussion based)** | **Table top/Command Post** | **Live play test** |
|---|---|---|
| Very few resources are required, and can be entirely internal. No disruption to business or staff. | More resources, planning and players are required. Can include external agencies. | Significantly more resource intensive to plan and deliver. |
| Can identify systematic issues in processes or gaps in processes/ policies/procedures. | Specific scenarios can be used and operational issues identified. | Allows all staff and stakeholders to practice their roles/responses and identify issues that other exercise types do not. |
| Does not address the effectiveness of processes, or allow staff to practice procedures. | Virtual nature can lead to practical issues not being identified, and does not test reality. | Greatest level of realism, providing confidence that plans are likely to work in a real no-notice event. |

**Remember:** the greatest vulnerability to any organisation is complacency

© NaCTSO Crown copyright 2017

## 5. LEGAL REQUIREMENTS

Management already has a responsibility under Health and Safety Regulations, Civil Contingency Act 2004, and the Regulatory Reform (Fire Safety) Order 2005 or in Scotland the Fire (Scotland) Act 2005 and Fire Safety (Scotland) Regulations 2006. The Management of Health and Safety at Work Regulations 1999 (the Management Regulations) generally make more explicit what employers are required to do to manage health and safety under the Health and Safety at Work Act.

As part of managing the health and safety for your business, you must control the risks in your workplace. To do this you need to think about what might cause harm to people and decide whether you are taking reasonable steps to prevent that harm. This is known as risk assessment and it is something you are required by law to carry out. If you have fewer than five employees you do not have to write anything down. What the law requires here is what good management and common sense would lead employers to do anyway: that is, to look at what the risks are and take sensible measures to tackle them. Having identified the threats and vulnerabilities, you then have to decide how likely it is that harm will occur, i.e. the level of risk and what to do about it. Risk is a part of everyday life and you are not expected to eliminate all risks but manage the main risks responsibly.

## 6. INSURANCE

Insurance against damage to your own commercial buildings 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 and customers caused by terrorism is achievable, albeit at a cost.

## 7. FURTHER INFORMATION AND ADVICE

For independent and impartial counter terrorism advice and guidance that is site specific, the security manager should establish contact with the local police Counter Terrorism Security Advisor (CTSA). Contact details are available through the NaCTSO website.

Your CTSA can:

- support you in assessing the threat, both generally and specifically
- give advice on physical security equipment and its particular application to terrorist attack methodology and comment on its effectiveness as with a deterrent, any protection and also aid a post-incident investigation
- facilitate contact with emergency services and local authority planners to develop appropriate response and business continuity plans
- identify appropriate trade bodies for the supply and installation of security equipment
- offer advice on search plans etc.

It is also advisable to consult with other occupants, partners, stakeholder, neighbours, emergency services and local authority.

ISO 31000, BS 31100 and ISO 31010 provide further guidance on risk management techniques.

Go to the Government Workplace fire safety webpage

Go to the NaCTSO website

Go to the Health and safety executive risk management webpage

**GO TO SECTION CONTENTS**

You may want to complete the Emergency and business continuity checklist

Go to Glossary

© NaCTSO Crown copyright 2017

# Threat level and building response plans

## 1. INTRODUCTION

The main threats to national security are terrorism, espionage, cyber threats and the proliferation of weapons of mass destruction, many of which impact on the UK's national infrastructure. Understanding the threat facing us is key to ensuring protective security measures and mitigations are proportionate, effective and responsive.

- Contact 999 to report an iminent threat
- Contact the Anti-Terrorist Hotline on 0800 789 321 to report suspicious activity
- Contact MI5 if you know something about a threat to national security such as terrorism or espionage

## 2. THREAT LEVELS

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. Those who own, operate, manage or work in crowded places are reminded that SUBSTANTIAL and SEVERE both indicate a high level of threat and that an attack might well come without warning.

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

Go to the Security Service (MI5) website

## 3. THREAT LEVEL DEFINITIONS

**The five levels of threat are:**

| | |
|---|---|
| **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 |

## 4. RESPONSE LEVELS

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

**The three levels of response are:**

| | |
|---|---|
| **Exceptional** | Maximum protective security measures to meet specific threats and to minimise vulnerability and risk – unsustainable |
| **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 protective security measures appropriate to the business concerned |

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

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

© NaCTSO Crown copyright 2017

To support your planning, the threat level and response levels are combined on the below table:

| Threat Level and Definition | Response Level | Description |
|---|---|---|
| **Critical**<br>An attack is expected imminently | Exceptional | Maximum protective security. CRITICAL measures to meet specific threats and to minimise vulnerability and risk |
| **Severe**<br>An attack is highly likely | Heightened | Additional and sustainable SUBSTANTIAL and SEVERE protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk |
| **Substantial**<br>An attack is a strong possibility | | |
| **Moderate**<br>An attack is possible but not likely | Normal | Routine protective security. LOW and MODERATE measures appropriate to the business concerned |
| **Low**<br>An attack is unlikely | | |

## 5. WHAT CAN I DO NOW?

- Carry out a risk assessment that is specific to your site or venue.
- Identify a range of practical protective security measures appropriate for each of the response levels. Consider the different attack types. Your local CTSA can assist.
- Regularly review the response level for your site or venue at security meetings.
- Clearly display signage informing staff of the building response level. This should not be displayed in public areas.
- Regularly train, test and exercise.

The counter measures to be implemented at each response level are a matter for individual premises or organisations and will differ according to a range of circumstances. All protective security measures should be identified in advance of any change in threat and response levels and should be clearly notified to those staff who are responsible for ensuring compliance. It is important to test and exercise your activity for each response level.

**GO TO SECTION CONTENTS**

Go to the NaCTSO website

Go to the CPNI website

Go to the Security Service (MI5) website

Go to Glossary

© NaCTSO Crown copyright 2017

# Communication

## 1. INTRODUCTION

Communication runs through the length and breadth of every organisation and communication regarding counter terrorism security should be no different. Consider how your organisation communicates about such issues during 'business as usual' times, but consider also how communication would work in a time of crisis or shortly after such an event.

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 website and/or publications to communicate crime prevention and counter terrorism initiatives.

You should consider a communication strategy for raising awareness among staff and others who need to know about your security plan and its operation. Good communication can have the effect of making staff and visitors more vigilant, whilst not instilling anxiety or concern in the everyday venue or site user.

This guidance also provides an introduction to the concept of security-minded communications, how professional communications can help deter terrorist attack and wider criminality whilst simultaneously informing, reassuring and potentially recruiting the normal user to assist.

Read more about Personnel security training and good practice

## 2. ATTACK PLANNING AND HOSTILES' USE OF INFORMATION

Those planning an attack typically conduct hostile reconnaissance. This information gathering is a vital component of the attack planning process; it is essential not only to plan an attack with confidence of success but also to continually adjust these plans and assess the likelihood of success.

Generally, the more sophisticated the attack the more complex the attack planning, and consequently the greater the information requirement and reconnaissance need.

Ultimately hostiles want to succeed at their attack, so they need certain, reliable and detailed information to be assured of this. This gives us an opportunity to deter them via the type and content of communications that are put disseminates to and during an event.

## 3. SECURITY-MINDED COMMUNICATIONS

Communications professionals have a critical role in the protective security of a venue or event. They can assist by:

- Denying hostiles the ability to obtain the information that is essential for their attack planning, in particular information available online.
- Deterrence messaging; creating a perception of failure of the reconnaissance or the attack itself because of the effective security measures in place (that will detect and hinder their operation).

These effects can be achieved because in the process of conducting hostile reconnaissance the hostiles are making themselves vulnerable. They are actively looking for and obtaining this essential information. This gives us an opportunity to ensure they cannot get the information they need and to also send deterrence messages that will adversely affect their perception of success.

### 3.1 Denying useful information

Hostiles are looking for detailed, credible and reliable information. One of the most effective actions that a communications professional can undertake is to ensure the site, venue or any contractors are not accidently providing this information to a hostile audience. For example, an exact site schematic, precise details of security equipment (e.g. number of, placement, make and model) or other interventions (e.g. number of security officers and patrol patterns). There is no need for the normal site user to know this information, so where possible, ensure the detail is removed. Hostiles will then need to put themselves at risk detection to obtain this information.

© NaCTSO Crown copyright 2017

### 3.2 Deterrence messaging - promoting effective security capabilities

Deterrence is a vital component of disrupting hostile reconnaissance and attack planning. However in many cases it is assumed that because protective security measures are in place they are, by default, deterring. However, this is not always the case and to get the most out of deterrence for a site requires proactively marketing protective security capabilities, to the hostile audience, across a range of communication channels.

Proactively communicating the effective security capabilities of the site may result in hostiles discounting the site as a target at the initial target selection phase (which may be conducted primarily online).

How an organisation provides its messages and evidence of these capabilities needs to be done carefully and thoughtfully. For example, being considerate of the normal site user and their perceptions of such messages. Ideally this should be reassuring and informative, and critically, convey the protective security without giving away detail that could be helpful to hostiles.

Ultimately what you are trying to achieve is to:

- Inform and reassure the normal user, demonstrating what is and has been done to help keep staff and visitors safe at your venue or event. Also to request their assistance 'you have a key role to play'.
- Deter the hostile (across a wide range of criminality). Showcase what you have and are doing to make it difficult for hostiles and criminals to operate and to detect them 'come here and you are likely to get caught!'

**Remember:** It is important to promote capabilities, where possible, use websites, video and pictures; social media is an excellent platform for this – to help provide credible evidence that these capabilities exist and work.

For further information on personnel security communications and disrupting hostile reconnaissance speak with your local CTSA

**GO TO SECTION CONTENTS**

Read more about Hostile reconnaissance

Go to the CPNI Personnel and people security webpage

Go to the CPNI Disrupting hostile reconnaissance webpage

Go to Glossary

© NaCTSO Crown copyright 2017

# Suspicious items

## 1. GUIDANCE FOR THE PUBLIC

When dealing with suspicious items:

- Do not touch
- Try and identify an owner in the immediate area.
- If you still think it's suspicious, don't feel embarrassed or think somebody else will report it.
- Report it to a member of staff, security, or if they are not available dial 999 (do not use your mobile phone in the immediate vicinity).
- Move away to a safe distance- Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out.

**Remember:** If you think it's suspicious, SAY SOMETHING

## 2. GUIDANCE FOR STAFF

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

**CONFIRM**, **CLEAR**, **COMMUNICATE** AND **CONTROL**.

**2.1 CONFIRM whether or not the item exhibits recognisably suspicious characteristics.**

The HOT protocol may be used to inform your judgement:

**Is it Hidden?**

- Has the item been deliberately concealed or is it obviously hidden from view?

**Obviously** suspicious?

- Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
- Do you think the item poses an immediate threat to life?

**Is the item Typical of what you would expect to find in this location?**

- Most lost property is found in locations where people congregate. Ask if anyone has left the item.
- If the item is assessed to be unattended rather than suspicious, examine further before applying lost property procedures.

**2.2 CLEAR the immediate area**

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

**2.3 COMMUNICATE – Call 999**

- inform your control room and/or supervisor
- do not use radios within 15 metres.

© NaCTSO Crown copyright 2017

**2.4 CONTROL access to the cordoned area**

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

**GO TO SECTION CONTENTS**

Contact 999 to report an imminent threat

Go to the Security Service (MI5) website

Go to Glossary

© NaCTSO Crown copyright 2017

# Good housekeeping

## 1. INTRODUCTION

Good housekeeping improves the ambience of your premises and reduces the opportunity for placing suspicious items or bags and helps deal with false alarms and hoaxes. Items left insecure on site, such as flammable liquids, tools, scaffolding poles and ladders, could be used by terrorists and criminals during an attack.

## 2. GOOD HOUSEKEEPING

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

- Avoid the use of litter bins in critical, sensitive or vulnerable areas such as near glazing, support structures etc. Make sure these areas are monitored by your CCTV operators. Make sure there is additional and prompt cleaning in these areas
- Review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location
- Use of clear bags for waste disposal makes it easier to conduct an initial examination for suspicious items
- Review the use and security of any compactors, wheelie bins and metal bins used to store rubbish within service areas, goods entrances and near areas where crowds congregate
- Your operations manager should have an agreed procedure in place for the management of contractors, their vehicles and waste collection services. The registration mark of each vehicle and details of its occupants should be known to the security staff or manager in advance
- Keep public, communal and external areas (such as exits, entrances, lavatories, service corridors and yards) clean, tidy and well lit
- Keep the fixtures, fittings and furniture in such areas to a minimum – ensuring there is little opportunity to hide devices
- Lock unoccupied offices, rooms and store cupboards.
- Ensure that everything has a place and that they are returned.
- Place tamper-proof plastic seals on maintenance hatches.
- Pruning vegetation and trees, especially near entrances, will assist in surveillance and prevent the concealment of any packages.
- Ensure that all staff are trained in bomb threat handling procedures, or at least have ready access to instructions, and know where these are kept.
- Review your CCTV system to ensure that it is working and has sufficient coverage both internally and externally.
- Ensure that first-aid kits and fire extinguishers are checked regularly and ensure that they have not been interfered with and used items replaced. (Are sufficient staff trained in first aid for a terrorist type attack?).
- Security managers should identify a second secure location for use as a control room as part of their normal contingency plans.
- Security systems reliant on power should have an Uninterrupted Power Supply (UPS) available. This should be regularly tested if it is identified that power loss could impact on the safety of the public.
- Ensure street vendors, cycle racks, lockers and bins do not impact upon evacuation routes, assembly areas, exits or entrances.
- Ensure cycle racks and lockers are placed away from crowded areas. Monitor with CCTV if necessary

You may also want to complete the Bomb threats checklist

**Consult with a security professional, such as a CTSA, regarding the design and placement of street furniture, lockers, bins, cycle racks etc.**

GO TO SECTION CONTENTS

You may also want to complete the Good housekeeping checklist

You may also want to complete the Bomb threats checklist

Go to Glossary

© NaCTSO Crown copyright 2017

# Improvised Explosive Devices (IEDs)

## 1. IEDS ATTACKS

Improvised Explosive Devices (IEDs) can be an effective weapon for terrorists.

### 1.1 What is an Improvised Explosive Device?

An IED is a 'home made' bomb. The main explosive charge in an IED may be made from Home Made Explosive (HME), they may still be as powerful as commercial or military explosives. Although an IED is 'home made', they can be highly sophisticated and very effective.

They can be delivered using the following methods:

- Radio Controlled IED (RCIED)
- Person Borne Improvised Explosive Device IED (PBIED)
- Postal device (delivered) – often a Victim Operated IED (VOIED)
- Vehicle Borne IED (VBIED)
- Under Vehicle IED (UVIED)
- Time bomb IED

Whilst a PBIED potentially affords a more flexible and penetrative delivery of a smaller explosive device, a VBIED may be capable of delivering a large quantity of explosives to a target causing a great deal of damage.

Dependant on the terrorist group, targets are generally selected to either inflict mass casualties, attract widespread media coverage or cause economic and psychological damage.

### 1.2 PBIEDs

There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

### 1.3 Postal devices

Read more about Mail handling

### 1.4 RCIED

An RCIED is anw IED initiated electronically via a wireless method consisting of a transmitter and receiver (i.e. personal mobile radio [PMR], mobile phone, cordless phone, pager etc.)

### 1.5 VBIEDs and UVBIEDs

Read more about Vehicle bombs

### 1.6 Time bomb

An IED initiated by a timer switch.

## 2. THE EFFECTS OF IEDS

The effects of an IED can be highly destructive. It is not just the primary blast that can be lethal but debris, such as broken glass and metal in the form of secondary fragmentation, can present a hazard a considerable distance away from the seat of the explosion.

Post blast disruption can last many weeks causing further economic damage and infrastructure problems.

If you think your site could be at risk from an IED there are physical and procedural mitigation measures that can be utilised to help reduce the risk.

## 3. SUICIDE ATTACKS

The use of suicide bombers is a method of delivering an explosive device to a specific location. Explosives can be delivered using a vehicle, plane or maybe carried or conceal on a person, in the form of PBIEDs and VBIEDs.

## 4. PROTECTIVE SECURITY MEASURES TO CONSIDER

Further detailed information is provided throughout this guidance. Many measures can be taken at no cost:

- Attacks may be preceded by reconnaissance or trial runs. Ensure that any suspicious behaviour is reported to the police.
- Effective monitored CCTV systems may deter a terrorist attack or identify planning activity.
- Ensure that no one visits your protected areas without your being sure of their identity or without proper authority.
- Use physical barriers to prevent a hostile vehicle from driving into your premises through pedestrian entrances, goods/service yards or underground areas.
- Deny access to any vehicle that arrives at your goods/service entrances without prior notice and hold vehicles

© NaCTSO Crown copyright 2017

at access control points until you can satisfy yourself that they are genuine.

- Wherever possible, establish your vehicle access control point at a distance from the protected site, setting up regular patrols and briefing staff to look out for anyone behaving suspiciously.

For further advice on searching and screening speak to your local CTSA

**GO TO SECTION CONTENTS**

Read more about Vehicle bombs

Read more about Mail handling

Go to Glossary

© NaCTSO Crown copyright 2017

# Vehicle bombs

## 1. INTRODUCTION – VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVICE (VBIED)

A VBIED is a vehicle that contains and delivers an explosive device to a target. The vehicle may be old or new, inexpensive or valuable, liveried or plain, blend into most situations and modified to prevent detection. VBIEDs can range in size from bicycles to cars, trailers, vans and large goods vehicles. VBIEDs have caused significant casualties and structural damage to buildings when left parked near to crowded places or buildings or driven into them by people intending suicide. Injuries and fatalities may be greater when items are added to the device like nails, or when structures and objects near the explosion shatter or fragment.

It is likely that terrorists will continue to try and carry out such attacks in the UK, these may be multi-layered attacks with firearms, weapons, vehicles, IED including VBIED, or any combination of these.

Any part of the following examples may indicate unusual or suspicious behaviour or characteristics of drivers/riders or vehicles:

### 1.1 Behaviour of the driver/rider is unusual

This may include:

- buying a vehicle for cash or without identity documents or using false or forged identity documents
- rapidly parking and leaving the vehicle
- showing signs of stress, or concealment of features, when buying or parking the vehicle or obtaining the IED components
- completing hostile reconnaissance before the event, to practice deployment and gauge public response

Read more about Hostile reconnaissance

### 1.2 Characteristics of the vehicle are unusual

This may include:

- appearing out of place, apparently abandoned, illegally parked, have hazard lights on or headlights left on
- contents appearing out of place, such as gas canisters, wires, or modified electrical items such as alarm clocks and mobile phones
- registration differing between licence plate and windscreen permits
- licence plates newly attached, or with obscured characters to avoid recognition
- modified vehicle shell, such as a different body structure or patched paintwork
- sitting low on the rear axle, if a heavy load is in the boot or under the back seat
- emitting smells such as gas or fuel
- smoke apparent in the vehicle

**Trust your instincts. If you suspect it, report it.**

Call 999 if there's an emergency

Contact the confidential anti-terrorist hotline 0800 789321

## 2. UNDER VEHICLE IMPROVISED EXPLOSIVE DEVICE (UVIED) GUIDANCE

Under Vehicle Improvised Explosive Devices (UVIEDs) are small explosive devices, typically attached to or placed underneath a vehicle and intended to kill or seriously injure the vehicle's occupants. Depending on the design, size and emplacement of the device, they may also result in injury or death of others in the immediate vicinity and/or damage to the surrounding property.

Any individual or organisation who may be targeted by terrorists or extremists should consider the risk of UVIEDs. This attack method is well known and has been utilised successfully by different groups on a number of occasions.

Being improvised, UVIEDs may come in a variety of shapes and sizes. Different containers and camouflage have been used and attempted, including but not exclusively, the use of plastic lunchboxes, metal piping or wooden boxes. Paint and grease may be used in an attempt to hide the device or the UVIED could be constructed to resemble a legitimate car part.

UVIEDs are likely to be placed in reasonably accessible locations as those placing them will typically be keen to install the device quickly.

© NaCTSO Crown copyright 2017

Historically, typical external locations include:

- attached to the bottom of a vehicle
- in front, on top of or behind a wheel
- attached to a wheel arch
- tied to an exhaust
- on the ground under a vehicle

This is not an exhaustive list. UVIEDs are most frequently attached using magnets or adhesive due to the speed of these methods. UVIEDs can feature a number of different triggers to devices.

**Remember:** If you suspect a UVIED, you should NOT touch it or the vehicle, and you should immediately move away and call 999.

Call 999 if you suspect a UVIED

### 2.1 Mitigation

Wherever possible, park securely. Make use of a lockable garage where available. If not available, park your vehicle in a well-illuminated location where neighbours and you can see it. Avoid a set pattern in daily business that could aid prediction of your vehicle's location wherever possible. This includes routes to/from work and times/days for shopping. Consider installing movement-based lighting systems, CCTV or fencing as deterrents.

### 2.2 Search and Detection

Do not rely solely on these security measures, checks should still be made. You may consider that checking your vehicle will draw attention to you; this is a possibility but must be weighed against the potential impact of a UVIED attack. There are other ways that attention can be drawn to you, but no other way to check for a UVIED.

- Check your vehicle first thing every morning; night time is when the vehicle is most vulnerable.
- Check if the vehicle has been left unattended at any time during the day; it can take only a few seconds to plant a device.
- Check the ground for any disturbance; this may indicate that the car has been approached or a device buried below.

Do not allow friends or family near the vehicle before you have checked it thoroughly and are satisfied in your own mind that there is nothing untoward or suspicious. Make yourself familiar with the underside of your vehicle, as this will help to detect any anomalies. This is particularly important for larger vehicles where the underside may be more complex and provide greater opportunities for concealment of devices. Photographs may assist memory if they are available at the time of inspection.

## 3. RESPONSE

If something is found then stay calm. Do not touch it or any part of the vehicle. Move yourself and anyone else well away from the vehicle. Keep others from approaching the vehicle if possible and safe to do so. Once at least 15m away call 999, ask for police and explain what has happened. Take cover behind a substantial structure such as a wall or building, avoiding glazed areas. Trust your instincts.

Call 999 if you suspect a UVIED

## 4. CONSIDERATIONS FOR SITE SECURITY MANAGERS

Understand the threat posed by vehicles entering or in close proximity to your site. Whilst the principal risk is likely to be posed by large Vehicle Borne IEDs (VBIEDs) with the potential to cause catastrophic damage to structures and mass casualties, the risk of vehicles with UVIEDs should also be considered. Limit and control vehicle access to your site as far as possible. Consider screening vehicles in accordance with your risk assessment.

A number of different technological options are also available. These range from pole-mounted mirrors and cameras, to permanent or temporary drive-over inspection systems (for use at site entrances) and vehicle mounted detection systems (for specific, high-risk vehicles). Equipment solutions should only be procured

© NaCTSO Crown copyright 2017

as a result of a robust risk assessment and analysis of the operational requirement, as a part of a holistic approach to security. In particular, choice of security measures should take account of the relevant risks (likelihood and impact) associated with UVIED and VBIED attacks.

Read more about Hostile Vehicle Mitigation (HVM)

Read more about Access control

GO TO SECTION CONTENTS

Read more about Suspicious items

Go to Glossary

© NaCTSO Crown copyright 2017

# Bomb threats

## 1. BOMB THREATS: PROCEDURES FOR HANDLING BOMB THREATS

The vast majority of bomb threats are hoaxes designed to cause alarm and disruption. As well as the rare instances of valid bomb threats, terrorists and others may also make hoax bomb threat calls to intimidate the public, businesses and communities, to draw attention to their cause and to mislead police. While many bomb threats involve a person-to-person phone call, an increasing number are sent electronically using email or social media applications. No matter how ridiculous or implausible the threat may seem, all such communications are a crime and should be reported to the police by dialling 999. It is important that potential recipients – either victims or third-parties used to pass the message – have plans that include how the information is recorded, acted upon and passed to police.

### 1.1. The bomb threat message

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are rare occurrences. Precise motives for hoaxing are difficult to determine but may include revenge, extortion, a desire to impress, or a combination of these and other less understandable motives. The vast majority of cases are hoaxes and the intent is social engineering, to cause disruption, fear and/or inconvenience the victim.

### 1.2. Communication of the threat

A bomb threat can be communicated in a number of different ways. The threat is likely to be made in person over the telephone; however, it may also be a recorded message, communicated in written form, delivered face-to-face or, increasingly, sent by email or social media (e.g. Twitter or Instagram, etc.). A threat may be communicated via a third-party, i.e. a person or organisation unrelated to the intended victim and identified only to pass the message.

### 1.3. Immediate steps if you receive a bomb threat communication

Any member of staff with a direct telephone line, mobile phone, computer or tablet etc. could conceivably receive a bomb threat. Such staff should, therefore, understand the actions required of them as the potential first response to a threat message.

If you receive a telephone threat you should:

- stay calm and listen carefully
- have immediate access to a checklist on key information that should be recorded
- if practical, keep the caller talking and alert a colleague to dial 999
- if displayed on your phone, note the number of the caller, otherwise, dial 1471 to obtain the number once the call has ended
- if the threat is a recorded message write down as much detail as possible
- if the threat is received via text message do not reply to, forward or delete the message; note the number of the sender and follow police advice
- know who to contact in your organisation upon receipt of the threat, e.g. building security/senior manager, as they will need to make an assessment of the threat

You may want to complete the Bomb threats checklist

If the threat is delivered face-to-face:

- Try to remember as many distinguishing characteristics of the threat-maker as possible.

If discovered in a written note, letter or as graffiti:

- Treat as police evidence and stop other people touching the item.

If the threat is received via email or social media application:

- Do not reply to, forward or delete the message.
- Note the sender's email address or username/user ID for social media applications.
- Preserve all web log files for your organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after).

© NaCTSO Crown copyright 2017

**Remember:** Seek advice from the venue security/operations manager as soon as possible.

Contact 999 and follow police advice

## 2. ASSESSING THE CREDIBILITY OF BOMB THREATS

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. This is a tactic used to place additional pressure on decision makers. Police will assess the threat at the earliest opportunity. When specific intelligence is known to police advice will be issued accordingly; however, in the absence of detailed information it will be necessary to consider a number of factors:

- Is the threat part of a series? If so, what has happened elsewhere or previously?
- Can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?
- Considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- If the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?
- Is a suspicious device visible?

## 3. ACTIONS TO CONSIDER

Responsibility for the initial decision making remains with the management of the location being threatened. Do not delay your decision making process waiting for the arrival of police. Police will assess the credibility of the threat at the earliest opportunity. All bomb threats should be reported to the police and their subsequent advice followed accordingly. It is essential that appropriate plans exist, they should be event and location specific. Venue options to manage the risk include:

### 3.1. External evacuation

Leaving the venue will be appropriate when directed by police and/or it is reasonable to assume the threat is credible, and when evacuation will move people towards a safer location.

It is important to appoint people, familiar with evacuation points and assembly (rendezvous) points, to act as marshals and assist with this procedure. At least two assembly points should be identified in opposing directions, and at least 500 metres from the suspicious item, incident or location. Where possible the assembly point should not be a car park. You may wish to seek specialist advice, which can help to identify suitable assembly points and alternative options as part of your planning. It is essential that evacuation plans exist; they should be event and location specific. Evacuation procedures should also put adequate steps in place to ensure no one else enters the area once an evacuation has been initiated.

The police will establish cordons depending upon the size of an identified suspect device. Always follow police directions and avoid assembly close to a police cordon.

### 3.2 Internal or inwards evacuation ('Invacuation')

There are occasions when it is safer to remain inside. Staying in your venue and moving people away from external windows/walls is relevant when it is known that a bomb is not within or immediately adjacent to your building.

If the suspect device is outside your venue, people may be exposed to greater danger if the evacuation route inadvertently takes them past the device. A safer alternative may be the use of internal protected spaces. This type of inwards evacuation needs significant pre-planning and may benefit from expert advice to help identify an internal safe area within your building. These locations should be in your plans.

If the location of the device threatened is unknown, evacuation represents a credible and justifiable course of action.

© NaCTSO Crown copyright 2017

**3.3 Decision not to evacuate or inwardly evacuate**

This will be reasonable and proportionate if, after an evaluation by the relevant manager(s), the threat is deemed implausible (e.g. a deliberate hoax). In such circumstances police may provide additional advice and guidance relating to other risk management options. It may be considered desirable to ask staff familiar with the venue to check their immediate surroundings to identify anything out of place, see search considerations below.

Read more about Evacuation, invacuation, lockdown, protected spaces

**3.4 Checking your venue for suspicious items – search considerations**

Regular searches of your establishment, proportionate to the risks faced, will enhance a good security culture and reduce the risk of a suspicious item being placed or remaining unnoticed for long periods. Additionally, if you receive a bomb threat and depending upon how credible it is, you may decide to conduct a 'search' for suspicious items. To that end:

- Ensure plans are in place to carry out an effective search in response to a bomb threat.
- Identify who in your venue will coordinate and take responsibility for conducting searches.
- Initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade.
- Divide your venue into areas of a manageable size for 1 or 2 searchers. Ideally staff should follow a search plan and search in pairs to ensure nothing is missed.
- Ensure those conducting searches are familiar with their areas of responsibility. Those who regularly work in an area are best placed to spot unusual or suspicious items.
- Focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points, car parks, other external areas such as goods or loading bays.
- Develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present.
- Under no circumstances should any suspicious item be touched or moved in any way. Immediately start evacuation and dial 999.
- Ensure all visitors know who to report a suspicious item to and have the confidence to report suspicious behaviour.
- Under no circumstances should any suspicious item be touched or moved in any way. Immediately start evacuation and dial 999.

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

**Remember:** it is vital that regular drills are carried out to ensure all are familiar with bomb threat procedures, routes and rendezvous points. Disabled staff should have personal evacuation plans and be individually briefed on their evacuation procedures. Similarly all visitors should be briefed on evacuation procedures and quickly identified and assisted in the event of a threat.

Contact 999 and follow police advice

© NaCTSO Crown copyright 2017

## 4. MEDIA AND COMMUNICATION

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide details of the threat, the decision making process relating to evacuation (internal or external) or why a decision not to evacuate was taken.

Releasing details of the circumstances may:

- be an objective of the hoaxer and provide them with a perceived credibility
- cause unnecessary alarm to others
- be used by those planning to target other venues
- elicit copycat incidents
- adversely affect the subsequent police investigation

**GO TO SECTION CONTENTS**

Read more about Search planning

Read more about Evacuation, invacuation, lockdown, protected spaces

Go to the NaCTSO website

Go to the CPNI website

Go to Glossary

© NaCTSO Crown copyright 2017

# Chemical, Biological and Radiological (CBR) attacks

## 1. INTRODUCTION

Chemical, Biological and Radiological material (CBR) attacks have the potential to cause significant harm and disruption, but they are difficult for terrorists to carry out effectively and weaponising often requires specialist knowledge and expertise.

To date, no such attacks have taken place in the UK. Alternative methods of attack, such as explosive devices, are more reliable, safer and easier for terrorists to acquire or use. Nevertheless, it is possible that a terrorist group may seek to use chemical, biological or radiological material against the West in the future.

**What is CBR?**

| | |
|---|---|
| **Chemical** | Poisoning or injury caused by chemical substances, including traditional military chemical warfare agents, harmful industrial or household chemicals. |
| **Biological** | Illnesses caused by the deliberate release of dangerous bacteria or viruses or by biological toxins, such as ricin, found in castor oil beans. |
| **Radiological** | Illness caused by exposure to harmful radioactive materials. |

Within the wider definition of CBR, the term 'White Powders' is also often used in a mail context to describe the potential presence of a noxious substance (or hoax material) in a letter or parcel that is designed to cause significant harm or disruption.

## 2. CBR MITIGATION

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

Full CBR protection can be extremely expensive to implement, however some measures that will mitigate to a certain extent the effects of a CBR event, can be put in place at relatively low cost. The following first steps are recommended to increase your resilience to a CBR attack:

- review the physical security measures relevant to areas of your building that may, due to their function (entrances, etc.), be at increased risk of attack
- review the design and physical security of your air-handling systems, such as access to intakes and outlets, avoiding the use of ground level, or near ground-level, air intakes
- ensure CBR response is featured into your site's major incident plans
- consider evacuation routes
- consider the use of pre-prepared messaging
- improve air filters or upgrade your air-handling systems, as necessary
- restrict access to water tanks and other key utilities
- review the security of your food and drink supply chains
- consider whether you need to make special arrangements for mail or parcels such as a separate post room, possibly with dedicated air-handling, or even a specialist off-site facility noting that mail rooms can be a high-risk area

© NaCTSO Crown copyright 2017

## 3. FURTHER INFORMATION

For further information on the strengths and vulnerabilities of your site or building in relation to CBR threats, contact your police CTSA. PAS 97: 2015 provides more detailed information and best practice for the screening of mail for 'white powders' and other threat items.

Note: For search and screening (as in many areas of physical security), knowledge of the target (such as threat material) is key to an effective search regime. Therefore an awareness of CBR is essential if this forms part of your search and screening process.

Contact your police CTSA

Go to PAS 97:2015

## 4. CBR RECOGNITION

As with other threat methodologies you may receive no prior warning of a CBR incident. Indeed the exact nature of the incident may not be immediately obvious.

First indicators may be:

- individuals showing unexplained signs of skin, eye or airway irritation, nausea, vomiting, twitching, sweating, disorientation, breathing difficulties
- the presence of hazardous or unusual materials/ equipment
- unexplained vapour, mist clouds, powder, liquids or oily drops
- withered plant life or vegetation
- distressed birds or animals.
- odd smells or tastes

**Steps 1, 2, 3** is a useful process to assist in the recognition of a CBR incident and a useful process to judge what actions to take:

| | |
|---|---|
| **Step 1** | One person in close proximity incapacitated with no obvious reason. Approach using existing security procedures. |
| **Step 2** | Two people in close proximity incapacitated with no obvious reason. Approach with caution using existing security procedures. |
| **Step 3** | Three or more people in close proximity, incapacitated with no obvious reason. **Do not** approach the scene – **stay away** – obtain further information, evaluate and immediately inform your security supervisor/security control room etc. |

The actions that are taken by building/site managers and security staff can, in the immediate moments following a CBR attack, have a very significant impact on limiting the effects of a CBR incident. Pre-planned actions focusing on limiting the effects of such an attack will help to ensure that building occupants are protected as far as is reasonably practicable.

In certain instances it should be possible to provide a list of 'immediate actions' that staff/security staff should follow, to both mitigate the effects of a CBR attack and to summon the relevant emergency services response.

Examples of actions which may be relevant include:

- Call the emergency services and follow their advice.
- 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 (i.e. away from the incident/source of contamination). If safe and practical to do so then the safe location should be selected so as to minimise spread of contaminants from the scene of the incident.

© NaCTSO Crown copyright 2017

- Consider removal of affected outer clothing, taking into account environmental conditions and the privacy of the affected person.
- Separate those directly affected by an incident from those not involved so as to minimise the risk of inadvertent cross-contamination.
- Ask people not to wander off – though you cannot contain them against their will.
- You do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties.
- When the emergency services arrive act upon their instruction as you may need further decontamination and medical help.
- 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.

The exact composition of the 'immediate actions' will vary from building to building and in some circumstances an action that may be appropriate for one building may be inappropriate for another. It is strongly recommended that users 'get to know their building' and procedures in preparation for developing a list of immediate actions. Consultation with your building services manager is essential if you are considering altering the state of your

HVAC system as part of a CBR response, as this may not be possible or appropriate.

In developing a CBR response strategy it is important to consider other emergency response plans (e.g. fire) that may already exist within your organisation to ensure there are no conflicts.

Read more about Evacuation, invacuation, lockdown, protected spaces

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Firearms and weapons attack RUN, HIDE, TELL

## 1. INTRODUCTION

Run Hide Tell – **stay safe**: Terrorist Firearms and Weapons Attack:

Firearms and weapons attacks are rare in the UK. The **'stay safe'** principles give some simple actions to consider at an incident and the information that armed officers may need in the event of a weapons or firearm attack:

### 1.1. RUN

- escape if you can
- consider the safest options
- is there a safe route? **Run** if not **hide**
- can you get there without exposing yourself to greater danger?
- insist others leave with you
- leave belongings behind

### 1.2. HIDE

- if you cannot **run, hide**
- find cover from gunfire
- if you can see the attacker, they may be able to see you. cover from view does not mean you are safe, bullets go through glass, brick, wood and metal
- find cover from gunfire e.g. substantial brickwork/heavy reinforced walls
- be aware of your exits
- try not to get trapped
- be quiet, silence your phone
- lock/barricade yourself in
- move away from the door

### 1.3. TELL

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

- location – Where are the suspects?
- direction – Where did you last see the suspects?
- descriptions – Describe the attacker, numbers, features, clothing, weapons etc.
- further information – Casualties, type of injury, building information, entrances, exits, hostages etc.
- stop other people entering the building if it is safe to do so

### 1.4 Armed police response

- follow officer's instructions
- remain calm
- can you move to a safer area?
- avoid sudden movements that may be considered a threat
- keep your hands in view

### 1.5 Officers may

- point guns at you
- treat you firmly
- question you
- be unable to distinguish you from the attacker
- officers will evacuate you when it is safe to do so

© NaCTSO Crown copyright 2017

**1.6 Plan and prepare now**

You must **stay safe:**

- what are your plans if there was an incident?
- what are the local plans? (personal emergency evacuation plan, first aid training etc.)
- consider first aid when it is safe to do so

**CitizenAID** is one example of a source of information for simple, clear teaching aid for immediate actions and first aid for a stabbing, bomb or firearms incident. Other guidance is available.

Be vigilant and to report any suspicious behaviour or activity.

Contact 999 if there is an emergency

Contact the confidential Anti-Terrorist Hotline on 0800 789 321

Go to CitizenAID

**GO TO SECTION CONTENTS**

Read more about Evacuation, invacuation, lockdown, protected spaces

Go to CitizenAid

Go to Glossary

© NaCTSO Crown copyright 2017

# Unmanned Aircraft Systems (UAS)

## 1. INTRODUCTION

Unmanned Aircraft Systems (UAS), also commonly referred to as drones or Remotely Piloted Aircraft Systems (RPAS), are aircraft that operate without a pilot being on-board. Rapid advances in small (under 25kg) Unmanned Aircraft System (UAS) technology represent a growing threat to the security of the UK. Cheap accessible electronics, advanced Global Positioning System (GPS) guidance, autonomous control, increasing payloads, lighter batteries, more efficient motors and a significant increase in reported incidents involving UAS reckless or negligent misuse have added to this anxiety.

The number of incidents reported at or around sensitive and iconic sites (including airports) and events throughout the UK is increasing. The UAS industry is forecast to be the greatest growth sector within the civil aviation industry over the next decade. There are a number of reasons why individuals seek to use UAS including non-malicious individuals who simply cause a 'nuisance'. The vast majority of operators have good intentions but their actions are sometimes seen as reckless.

## 2. MISUSE OF UAS

| | |
|---|---|
| **Danger to civil aircraft** | caused by UAS intrusion over airport real estate or on approach to an airport. |
| **Local smuggling** | of banned goods into closed establishments such as prisons |
| **Protest groups** | use of UAS to invade privacy or disrupt an event |
| **Journalism** | a UAS is used as a platform to record images/video of a site/incident from a good vantage point, usually external to the site |
| **Espionage** | to covertly collect sensitive information from a site that may reveal operational capabilities |
| **Physical attack** | a terrorist seeking to use a UAS to mount an attack against a site e.g. carrying an improvised explosive or chemical/biological device |
| **Hostile reconnaissance** | to support acts of terror, e.g. an actor seeks to collect information about a site that may then be used to develop an attack plan or protest action |

© NaCTSO Crown copyright 2017

## 3. ASSESSING THE RISK

Terrorists very often undertake some form of reconnaissance prior to carrying out an attack. Terrorists will survey a target or location to identify gaps or weaknesses. In recent years UAS have become increasingly more sophisticated.

In a period of heightened alert, it is vital to remain vigilant, trust your instincts and report possible reconnaissance to the police. When the use of a UAS is involved, the three main considerations in assessing potential preparatory activity are:

- the likelihood of a venue being targeted
- the type of suspicious activity shown
- why you think it is suspicious

## 4. PROTECTIVE SECURITY CONSIDERATIONS

Remember, you are the expert in your own working environment. The following advice is how you can control the situation in the event of a UAS incident and explain practical considerations for a guard force.

- **D**etect the drone
- **A**ssess the situation
- **L**ocate the pilot
- **E**ngage the pilot and control the situation
- **C**onsider further action

### 4.1 Detect

- visually locate the drone and alert colleagues
- observe its behaviour
- is it suspicious?
- is it carrying anything?
- is it a danger?
- is it filming?
- is it a nuisance?
- is it targeting a particular location?
- can you establish where it has come from?
- if landed or crashed, stay with drone until pilot arrives
- follow procedures for preservation of evidence

Note: Consider the presence of an Improvised Explosive Device (IED) if the UAS is seen to be carrying an object. Based on your initial assessment, do not approach or touch the UAS, evacuate people to a safe distance.

### 4.2 Assess the situation

Before engaging with the pilot or if pilot is not located, consider:

- is it a nuisance/threat?
- talk to person who reported the alleged incident
- talk to witnesses
- are there casualties or damage to property or immediate risk to life?
- should the pilot have written permission from the CAA or landowner?
- think safety first; your actions are likely to be filmed
- is there immediate risk to life?
- is it a sensitive or important site asset?
- does it pose a security risk?
- is the drone there to provoke a response?

### 4.3 Locate the Pilot

Consider the following:

- within 150m of the UAS
- two hands on control device
- have a good vantage point/line of sight
- using a smart phone, tablet, transmitter or a laptop
- looking towards the UAS
- something to transport the UAS
- may be surrounded by onlookers
- may have a crowd around them
- may be static or walking
- behaviour significantly different to others around them
- may be wearing First Person View (FPV) goggles

### 4.4 Engage the pilot control the situation

- Do not attempt to take control of the aircraft unless there is a serious threat to life and security. Consider waiting for the UAS to run out of power (20-30 minutes is typical).

© NaCTSO Crown copyright 2017

- be professional – camera footage from UAS is often posted on the internet
- be proportionate – many UAS operators do not know the law and do not aim to intentionally break the law
- instruct the pilot to land the aircraft in the safest and fastest way
- request the transmission or control and the aircraft be switched off

**4.5 Consider further action**

- An offence is committed if a UAS equipped with a camera is flown within 150m of a Congested Area, within 150m of any open air assembly of more than 1000 people and within 50m of any person or thing not under the control of pilot – without written Permission of the CAA (Air Navigation Order (ANO) 2016 Article 95).
- UAS must not endanger any person/property (Article 241 ANO 2016).
- UAS may be flown legally if they do not carry a camera. However, the pilot must ensure the flight can safely be made, they maintain unaided visual contact with the device and they do not drop anything from it that can cause harm or damage. (Article 94 ANO 2016).
- Congested area in relation to a city, town or settlement. (Any area which is substantially used for residential, industrial, commercial or recreational purposes-Article 255 ANO 2009).

## 5. DETERMINE

- why the pilot is flying in the area and what they are seeking to achieve?
- if the UAS has a camera and if it is recording?

## 6. DETER

The use of signage (portable and fixed) prohibiting the use of UAS at key points and vulnerable areas sends out a powerful deter message. Police action is now supported and informed by detailed guidance. Some airports have implemented local response and prosecution strategies. Promotion of prosecutions may have a powerful deterrent effect.

Awareness raising campaigns are carried out the Civil Aviation Authority (CAA), using their material will support your efforts.

## 7. DISRUPT AND DENY

Physical barriers (nets, wires etc.) have limitations.

## 8. DO GENERAL MEMBERS OF STAFF KNOW WHAT TO DO/HOW TO REPEAT A SIGHTING OF A UAS?

**8.1 Do your staff know what to do if:**

- A member of staff or visitor reports the occurrence of a UAS?
- They spot a UAS in flight?
- They find or recover a UAS (such as a crashed UAS) within the site.
- They find or recover a UAS adjacent but external to t8.2.

**8.2 Do security staff:**

- Know the locations where a UAS is most likely to be controlled from?
- What to do if they locate the pilot, whether they are within or outside of the area of land owned by the site?
- Are the procedures appropriate if the threat from UAS increases?
- Is a system in place to assess the impact of any compromises that may have occurred (such as to assess the impact of a loss of sensitive information)?
- Are the policies/procedures compliant with the law?

**8.3 It is recommended that the development of procedural responses is carried out in consultation your CTSA and any other key stakeholders.**

Practical considerations for the guard force:

It is most likely that UAS flown within/near to a location will be controlled by individuals who may not have malicious intent. Furthermore, the UAS used are most likely to be flown by pilots who have line of sight to the aircraft. Consequently, it is recommended that asset owners conduct a vulnerability survey to identify the

© NaCTSO Crown copyright 2017

most likely locations where a UAS will be set up for flight and where a pilot is likely to be located. This information should then be utilised within a security control room and command structure to attempt to locate a pilot should the presence of a UAS be detected.

## 9. HANDLING UAS

- try and preserve for evidential value
- minimal handling, think forensics (consider Improvised explosive device IED)
- do not remove the batteries or memory card
- switch it off and package appropriately (place in a box)
- consider storage (do not store in a control room as it may still be recording)
- think about your own safety
- if in doubt seek advice from your local police

In an emergency call 999

## 10. PHYSICAL MITIGATIONS

The selection of the most appropriate physical mitigations will depend upon the nature of the risks. Depending on the risks, you may wish to consider:

- For new builds, locating the most important assets as far away from the perimeter as possible. This can be useful for managing other types of risks, such as forced entry incursions, vehicle borne improvised explosive devices etc.
- Using 'cover from view' screens around the building, perimeter, or at the most vulnerable locations, to make observation from outside more difficult. This can include using foliage, non-transparent screens fitted to fencing, blinds in windows and the like, but consideration should be given to any implications on safety, other security measures (e.g. CCTV) or operational responses.
- Concealing/disguising the asset to make it more difficult to locate and identify.
- Protecting the asset, by placing a physical barrier around it. For example, locate it within a building or if out in the open, use a net/grillage to prevent close access etc. Any openings in the 'enclosure' should be designed so that it would be difficult for a UAS to exploit.
- For sensitive assets or sensitive information stored within buildings, consider using obscuration film and/or blinds fitted to windows. Similarly the internal arrangement of rooms may be reconfigured to reduce the vulnerability (e.g. move computer screens so that they cannot be observed from outside of the building).

## 11. DETERRENCE COMMUNICATIONS

Nearly all terrorist attacks involve reconnaissance and it is possible to both frustrate and deter attack planning during this phase by using a range of communication tools – this is referred to as deterrence communications.

Go to the CPNI website

## 12. PERSONS RECEIVING REMUNERATION FOR THEIR WORK

Anyone operating a small unmanned aircraft (20kg or less) for Commercial Operations and receiving remuneration requires permission to operate from the CAA. Such operators of small unmanned aircraft being used to film close to people or objects also require permission from the CAA, whether or not they are undertaking aerial work. Specifically, this means flight over or within:

- 150 metres of any congested area.
- over or within 150 metres of an organised open-air assembly of more than 1,000 persons
- flight within 50 metres of any person, vessel, vehicle or structure not under the control of the pilot

To obtain these permissions, an operator has to prove a sufficient level of competence and an understanding of the safety. Pilots must maintain direct unaided visual contact with the small unmanned aircraft at all times. Within the UK, such 'visual line of sight' operations are normally accepted to a maximum distance of 500m

© NaCTSO Crown copyright 2017

horizontally and 400ft vertically from the pilot. In this context, 'unaided' does permit the use of corrective spectacles. Flight beyond these distances can be permitted, but the operator is required to provide explicit proof that this can be conducted safely.

Project Griffin provides National Counter Terrorism Awareness advice which includes information on dealing with UAS:

- **IF YOU SUSPECT IT, REPORT IT**
- **CALL 0800 789 321 CONFIDENTIAL ANTI-TERRORIST HOTLINE**
- **IF URGENT DIAL 999**

Call the confidential anti-terrorist hotline 0800 789 321

Call 999 in an emergency

Go to the CAA UAS webpage

Go to the NaCTSO website

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Vehicle as a weapon

## 1. INTRODUCTION

The threats from vehicles range from vandalism to sophisticated or aggressive attacks by determined criminals or terrorists. As well as a convenient method to deliver an improvised explosive device an additional attack methodology is using a vehicle as a weapon (VAW).

A vehicle by itself can also be used with hostile intent to breach a perimeter, ram and damage infrastructure, or as a weapon to injure and kill people.

This is referred to as a 'vehicle as a weapon' attack. The use of a vehicle as a weapon is a low complexity methodology and has been used by terrorists to target crowded places. A broad range of vehicles can cause significant loss of life and serious injury.

Attacks using vehicle as a weapon requires little or no training thus are within the capability of most individuals. Online terrorist media continues to inspire and incite individuals to use a vehicle as a weapon as an attack.

**GO TO SECTION CONTENTS**

Read more about Vehicle bombs

Read more about Hostile Vehicle Mitigation (HVM)

Read more about Guidance for commercial vehicles and hire companies

Read more about Evacuation, invacuation, lockdown, protected spaces

Go to Glossary

© NaCTSO Crown copyright 2017

# Physical security introduction

## 1. INTRODUCTION

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

With appropriate planning physical measures, to remove or reduce your vulnerabilities, bear in mind the need to consider safety and emergency response as a priority at all times.

Effective physical security of a crowded place is best achieved by multi-layering the different measures, what is commonly referred to as 'defence-in-depth'. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer. Each layer of security may be comprised of different elements.

In order to achieve success an adversary will attempt to identify and exploit weaknesses within your protective security measures. The CPNI principles of Deter, Detect and Delay supported by an effective response plan will help to frustrate and disrupt an attacker.

Considering the physical security requirements at the outset as part of the venues planning and design phase will often result in more effective and lower cost security. Your risk assessment will determine which measures you should adopt. It is essential that you understand the threats faced by your venue or site; effective security depends on a proportionate alignment to the threat.

Go to the CPNI website

## 2. OPERATIONAL REQUIREMENTS

The Operational Requirements process helps organisations make smarter investments in security, enabling them to implement measures which are in proportion to the risks they face. By following the process security managers and practitioners are able to assess, develop and justify the actions their organisation needs to take, and the investments they need to make to protect critical assets against security threats.

Go to the CPNI Operational Requirements webpage

## 3. SECURITY AWARENESS

Vigilance by staff and visitors at all crowded places is essential to your protective measures. Staff will know their own work areas well and should be encouraged to be alert to unusual behaviour or items that are out of place. They must have the confidence to report any suspicions, knowing that reports, including false alarms will be taken seriously.

### 3.1 Training

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, unusual interest shown by strangers in less accessible places and suspicious behaviour.

Read more about Hostile reconnaissance

Read more about Personnel security training and good practice

### 3.2 Deterrence

Hostiles will not necessarily be automatically deterred from a crowded place simply because it has CCTV, guards or a particular fence or lock. Instead, an organisation needs to use these security measures in an effective manner. Effective security measures with an alert and professional guard force and staff will require hostiles or criminals to conduct further attack planning and pose an extra risk of detection, which they may be unwilling to accept. If a hostile assesses a site has excellent security measures due to the information available online, on a poster or witnessed in operation, it may be enough to deter them from their target altogether.

Read more about Communication

### 3.3 Patrolling, guarding and security officers

Routine searching and patrolling of premises represents another level of security and may cover both internal and external areas. Ensure patrols are carried out regularly but at unpredictable times. Staff must have clearly defined

© NaCTSO Crown copyright 2017

roles and responsibilities, tasking and procedures to follow. This must be underpinned by training, rehearsal and exercising.

Read more about Personnel security training and good practice

## 4. ACCESS CONTROL

Controlling access into a site or venue may include either people, items or vehicles and is an essential layer of protective security. An efficient entry system benefits the smooth flow into a crowded place. Ensure that the boundary between public and private areas of your venue are secure and clearly signed. Ensure there are appropriately trained and briefed security personnel to manage access control points.

Consideration should be given to how vehicle access could be controlled at the point of entry, particularly searching or screening of vehicles in response to a specific threat. Larger sites may additionally have 'crash' gates that will require a strict security regime to ensure they are not breached. Access points should be kept to a minimum, with any boundary fences or demarcation lines clearly signed.

Read more about Search planning

Access control systems and locks are designed to control who can go where and when. These systems integrate with physical barriers to provide delay and detection against a multitude of attackers. Controlling access can be done via:

- Automatic Access Control Systems (AACS) that control a number of doors across a single or multiple site
- locks (electronic or mechanical) that control access to a single door

Consideration should be given to investing in good quality access control systems that are not only physically robust but also cyber secure.

Read more about Access control

### 4.1 Key management

Read more about Access control

### 4.2 Security passes

Read more about Access control

## 5. THE PERIMETER

There should be measures in place to ensure that a venue or site can exercise a degree of control over the activities that take place within their property boundaries. Defensible space is created by deciding which areas around a property are public and which areas are private. Simply put, boundaries should clearly define the difference between public and private space. This is particularly important when challenging protests and unlawful activity. There should be measures in place to ensure that an occupier can exercise a degree of control over the activities that take place within their property boundaries.

### 5.1 Fencing

Fencing is often used as a perimeter providing a line of demarcation, it is an important security measure, both for deterring criminal activity and enhancing safety. Once installed, it should be regularly checked to ensure that it is in good repair and fit for its intended purpose. Perimeter intrusion detection systems, may be used at the perimeter to alert security officers that the perimeter has been breached.

### 5.2 Hostile Vehicle Mitigation

Your CTSA will be able to advise you.

Read more about Hostile vehicle mitigation

## 6. CONTROL ROOMS

Security Control Rooms (SCRs) form the hub of a site's security. The control room's main function should be security, non-security responsibilities should be discouraged. Control room setup should allow serious incidents and crisis situations to be handled without compromising the ability to deliver normal security functions.

© NaCTSO Crown copyright 2017

Seek specialist advice and refer to the CPNI website.

Go to the CPNI website

## 7. STRUCTURAL FRAMING, WALLS AND FLOORS

Buildings within the UK are usually constructed using a structural frame, typically steel, concrete or timber, or are built from unframed masonry. There are many different types of walls and floor systems that are used within buildings, but together these elements play an important role in protecting occupants and assets from the effects of blast and other security threats. For many, a primary security concern is for the building to remain standing, or for damage to be limited to defined zones, following an attack involving explosives, impact and/or fire.

Designing structural framing, walls and floors for structures so that they incorporate physical security requirements from the outset will help deliver robust and resilient business operations. Where it is necessary to retrofit or adapt existing structures, physical security needs should form a central part of the requirements definition process for the enhancements.

Go to the CPNI website

Go to the BRE website: redbooklive.com

## 8. EXTERNAL DOORS AND WINDOWS

Good quality external doors and windows are essential to ensure building security. Advice on standards are available the Secure by Design or CPNI websites or local CTSAs. Consideration should also be given to intruder detection systems. 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 involving explosive devices are caused by flying glass. 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 the shattering effect and therefore reduce the possibility of casualties. 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 CTSA.

Working from a security threat and risk assessment it should be determined which of the following types of attack the door and windows need to work against:

- blast
- ballistic – people either trying to shoot at occupants through the door or to damage the door/door hardware in order to gain entry
- manual forced entry – attackers using tools to try and force entry through the door
- surreptitious entry – an attacker trying to infiltrate through the door leaving no indication of compromise

Contact your local CTSA for advice on standards

Go to the CPNI website

Go to the Secured by Design website

Go to the BRE website: redbooklive.com

### 8.1 Doors

Doors form an essential part of physical security and are often required to perform several functions, including to:

- control access for authorised personnel
- permit an appropriate flow of people/materials etc.
- work in conjunction with intruder detection systems (IDS), to detect unauthorised access
- provide a barrier to delay the progress of an adversary
- provide protection from specific types of threat, such as blast or ballistic
- provide protection from fire and/or smoke ingress
- provide a means of escape in an emergency

Security doors should also integrate with sensors for intrusion detection and access control systems. Whether they are part of the external façade, or form part of the boundary around a space within the building, it is important to define the security requirements for each door.

© NaCTSO Crown copyright 2017

### 8.2 Windows

Windows comprise of a number of components and their security resistance is linked to how these components perform as a system. Consequently, when specifying the level of protection required of the window, it should relate to the whole system, not just the glass. When identifying glazing there are various types of glass to select from, each of which has different properties:

- Annealed/float glass – traditional window glass which forms sharp glass shards when broken. It is not recommended for use in any security solution.
- Toughened glass, also known as tempered glass – the production process produces glass that is approximately five times stronger than annealed glass. It will break into small chunks instead of glass shards
- Heat strengthened glass – this is similar to toughened glass but is only twice the strength of annealed glass.
- Laminated glass sandwiches – an interlayer between layers of glass designed to hold together when the glass shatters.
- Polycarbonate – significantly stronger and lighter than glass and hard to break

Laminated glass is the preferred option for most security applications because of its unique properties. Care should be taken to ensure that the correct type of laminate is specified and used. It is also important to ensure that the rest of the glazing system, e.g. support structure and fixings, are specified correctly.

Anti-shatter film and bomb blast net curtains may be used in conjunction with any of the types of glazing. Additional measures such as bars and grilles may also be incorporated to provide enhanced security. Thought should be given to whether these are placed inside or outside the glazing. Obscuration measures can be used to mitigate both the threat of ballistic attacks and unauthorised observation. In the case of ballistic attacks, such measures will prevent aimed shots but may not stop un-aimed fire. Therefore, the construction details of glazing needs to be considered to determine whether they will withstand bullets from the selected threats.

## 9. HEATING, VENTILATION AND AIR CONDITIONING SYSTEMS (HVAC)

In order to maintain a comfortable indoor environment, occupied buildings will feature some form of ventilation and heating or cooling. This may be achieved through natural ventilation, mechanical ventilation (e.g. fans/ blowers) or hybrid ventilation systems.

Modern, commercial buildings such as shopping centres, airport terminals and sports venues typically use a distributed (mechanical) heating, ventilation and air-conditioning (HVAC) system. HVAC systems, which can have many points of access, potentially provide a viable, rudimentary means of dispersing chemical or biological agents, and so consideration of measures to reduce this risk may need to be considered:

- review the design and physical security of your air-handling systems, such as access to intakes and outlets
- improve air filters or upgrade your air-handling systems, as necessary.

Read more about CBR attacks

## 10. 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.

Read more about CCTV

### 10.1 Alarms

The National Police Chief Council (NPCC) security systems policy (www.securedbydesign.com) sets out the police requirements for alarm systems installed by compliant companies to gain a police response to your premises. Compliant companies can apply for a police Unique Reference Number (URN) which is used to identify your individual security system within the police database to

© NaCTSO Crown copyright 2017

ensure your alarm activation has an immediate response. Ensure that your security system company is police compliant and they can supply a URN.

NPCC require security systems companies to be certified by an inspectorate accredited by the United Kingdom Accreditation Services (UKAS) to EN 45011 and to relevant British Standards listed in the NPCC security systems policy. The two inspectorates approved by the NPCC are: National Security Inspectorate (NSI) and Security Systems and Alarms Inspection Board (SSAIB).

Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations.

Go to the NSI website

Go to the SSAIB website

Go to the Secured by Design website

**10.2 Lights**

External lighting provides an obvious means of deterrence as well as detection, but take into account the impact of additional light pollution 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.

Read more about CCTV

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Evacuation, invacuation, lockdown, protected spaces

## 1. INTRODUCTION

### 1.1 Requirement for guidance

Managers of crowded places now have to consider a wider range of terrorist methodologies than previously, including hostile actors using firearms and vehicles as weapons. This wider range of threats to safety of people in crowded places requires a range of "emergency responses" including emergency evacuation, "invacuation" (inward evacuation), lockdown, and use of protected spaces.

This document is intended to provide guidance to the Security Manager or individual(s) assigned responsibility for crowded places in planning, deciding on and implementing their emergency response. Other guidance outlines to members of the public and individual members of staff to help them prepare for these emergency scenarios.

This document provides generic advice for all crowded places: venues, buildings and events.

### 1.2 Responsibility for deciding emergency response

The initial decision-making regarding emergency response is usually made by the management of the crowded place. Initial decision-making should not be delayed in order to wait for instruction or action from the police. Speed of decision-making and implementation are critical.

Police will assess the threat or attack at the earliest opportunity and provide support, advice and guidance when they are able to do so. In exceptional cases the police may insist on evacuation, although they should always do so in consultation with the Security Manager or responsible individual.

Actions should be reasonable, necessary and proportionate based upon the circumstances, particularly when they are necessary to protect life and limb. You should always record and justify your actions.

### 1.3 Requirement for planning

Crowded places should have a security plan, the objective of safeguarding staff, visitors, and contractors from potential hazards. In terrorism scenarios planning should be designed to promote the highest chances of staff, visitor and responder survivability. Measures to detect, deter and delay attackers, and planning for various emergency responses, will improve survivability.

### 1.4 Managing in Crisis and Requirement for Training and Rehearsal

A key challenge is being able to respond effectively in a confusing and potentially life-threatening situation.

Following a threat, or during an attack, it is unlikely that anyone will understand its full extent or be able to predict how it will unfold.

The normal staff structure may not be in place. Familiarising staff with responses to different threat and attack scenarios and their associated indicators (such as gun shots, communication from patrolling guard force, observations from CCTV etc.) can increase the likelihood that they will be able to respond correctly and quickly. As some scenarios develop staff will make their own decisions e.g. Run, Hide, Tell.

Training and rehearsal is crucial. It will aid managers and their teams to identify how to respond most effectively and facilitate speed of decision-making and implementation, which is critical to promoting survivability in these scenarios. Leadership is a key attribute, training and rehearsal will enable individuals to make dynamic risk assessments and respond effectively.

### 1.5 Emergency response planning should be based on SIX key actions

These responses support the objective of promoting the highest chances of staff, visitors and responder survivability:

1. Appoint a designated individual to prepare a security plan, train and rehearse.
2. Evaluate the credibility or extent of a threat or attack.
3. Report the incident to police and alert people within the site/location.

© NaCTSO Crown copyright 2017

4. Decide on appropriate response. Establish if the threat is external or internal to the venue. If it is within the venue consider evacuation, but if the threat or incident is outside the venue it may be safer to stay inside. Initiating evacuation, invacuation, lockdown and/or use of protected spaces should be the responsibility of the responsible individual.
5. Instruct staff, visitors, and contractors – what they should do and where they should go.
6. Deter people from entering the area. Reduce the number of potential causalities by trying to prevent people entering the venue or site.

**1.6 Terminology**

For a list of definitions see Glossary

## 2. RESPONSE PLANNING

When planning, it may be useful to consider the response in three phases:

Phase 1. Pre-incident (Think ahead)

Phase 2. Incident (Consider your options and Take Action)

Phase 3. Post Incident (Recovery)

Appendix A and Appendix B summarise factors for consideration during an emergency for organisations (A) and individuals (B).

Appendix C : Planning considerations for each attack type to support an evacuation/invacuation/lockdown.

**2.1 Pre-Incident – Think ahead**

**2.1.1 Develop a plan**

- Ensure an individual, with a designated deputy(-ies), is responsible for the plan and its delivery.
- Anticipate potential threats and assess the risks.
- Develop response plans specifically for each site/ location, possibly including individual buildings or spaces within the venue, and co-ordinate with neighbours.

**2.1.2 Ensure your crowded place infrastructure facilitates your plan**

Ensure your infrastructure supports procedures for emergency response as necessary according to your plan; e.g. signage to identify specific emergency evacuation routes, remote control of vehicle shutters, CCTV etc.

**2.1.3 Prepare and train your personnel (staff, security, contractors and visitors where appropriate)**

- Awareness of the threats (consider Project Argus and Project Griffin).
- Create a strong security culture, including reporting of incidents.
- Develop Standing Operating Procedures (SOPs), and reflect in training.
- Ensure roles and responsibilities are clear and understood.
- Training, exercising and rehearsal (in person, on-line). Familiarise staff with all evacuation routes (including outside buildings, sites, events or away from the crowded place) and assembly points, if applicable. Some rehearsals should prohibit the use of one or more evacuation routes so that staff and contractors become familiar with alternative routes.
- Floor plans- ensure they are accessible to key staff.
- Prepare crisis response kits.
- Ensure reference material is available to staff (checklists, pocket cards, posters).

You may want to complete the Crisis response kits checklist

**2.1.4 Deny, deter, and detect hostile reconnaissance**

- Ensure staff remain vigilant, making the operating environment hostile. Demonstrate a strong security posture through visible and effective activity, such as, by staff awareness and reporting processes, effective use of CCTV and deterrent communications.
- Intervene to prevent the threat.
- Notify the appropriate authorities.
- Record your actions.

Read more about Hostile reconnaissance

**2.1.5 Detect attackers**

- actively monitor news channels and CCTV
- ensure good communications with neighbours
- consider alarm call points at strategic locations

© NaCTSO Crown copyright 2017

- consider attack detection systems (e.g. sound/firearms)

Seek advice from CPNI

Seek advice from your local CTSA

**2.2 Incident - Consider Your Options and Take Action**

- Report any incident to the police as soon as possible to initiate an appropriate response.
- Stay calm and assess the situation. Establish what response, if any, is required, including for example, the safest place(s) and/or route(s).
- Police will assess the credibility of the threat at the earliest opportunity. Police will require different information for different scenarios.

You may want to complete the ETHANE checklist

**2.2.1 Delay attack or threat and protect most important assets.**

Consider:

- How to cause the attackers to waste time, energy, ammunition and weapons on overcoming barriers and not targeting personnel; e.g. use of 'Active Delay Systems' at specific locations to confuse, disorientate and slow the attacker and/or control use of lifts, escalators and stairwells.
- How to maximise the opportunity for staff, visitors and responders to survive.
- How to maximise the opportunity to protect critical assets.

Seek advice from your local CTSA

Go to the CPNI Active access delay systems webpage

**2.2.2 Respond and manage the incident**

- Consider empowerment of security officers vs. centralised control: the best picture is often from the ground.
- Locate, track and monitor intruders/hostiles (e.g. via CCTV etc.) and communicate information to police.
- Open and maintain communication between buildings, occupants and emergency services – using prepared communication templates, with the option of multiple modes of communication.
- Consider evacuation, invacuation (possibly to a protected space) and/or lockdown.
- Implement emergency response and instruct staff, visitors and contractors.
- Deal with the injured when it is safe to do so.
- Staff and visitors may have different responses to the same incident. Managers should consider the impact of staff, contractors or visitors not following or directly contradicting instructions.
- Have immediate access to key checklists for procedures and key information that should be recorded.
- Record and justify your actions.

Go to CitizenAID

**2.3 Post Incident: Recovery**

Recovery and resumption to normal operations – managing the consequences of a threat or attack.

Organisations should remain vigilant in case circumstances change. Once it is established that there is no longer a threat, organisations should engage in post-incident assessments and activities, including:

- Accounting for all individuals at designated assembly point(s), through contact with staff, or via business continuity systems, to determine who, if anyone, is missing and potentially injured.
- Assessing the psychological state of individuals at the scene, and referring them to health care specialists accordingly (long term maintain a period of 'watchful waiting' for a month post incident).
- Notifying families of individuals affected by the incident, including notification of any casualties.
- Recording actions.
- Identifying and filling any critical personnel or operational gaps left in the organization as a result of the incident.
- When appropriate, identifying "lessons learned" and incorporate into training and rehearsal.

© Crown copyright 2017

## 3. TYPES OF EMERGENCY RESPONSE

There are a number of options for emergency response including:

- a full site evacuation
- a phased evacuation (consider if you require dedicated searchers to remain)
- partial or zonal evacuation
- a directional evacuation, in which staff, contractors and visitors are directed to specific exits and routes
- an invacuation to safer areas, including protected space(s), if available
- a partial invacuation
- no action is required (a decision is made not to evacuate or invacuate)
- lockdown

**3.1 Full site evacuation**

Leaving the crowded place will be appropriate when directed by police and/or it is reasonable to assume the attack or threat is credible, and when evacuation will move people towards a 'place of relative safety'. You may wish to 'evacuate to the nearest exit' or direct people to specific exits.

Knowledge of the approximate time to evacuate (from testing and exercising and analysis including crowd modelling) and time for individuals to navigate the route should inform decision-making and instructions to staff. The safety of particular routes may change during the course of an attack. For example: use of lifts (in non-fire scenarios) may reduce evacuation times but send people to the lobby area where attackers may be located.

**3.2 Directional evacuation**

A directional evacuation should be used if a specific area is currently, or may become, dangerous or a given route would result in people passing through or near to the area of the threat. Selection of this strategy might increase evacuation time but improve safety.

It requires staff and visitors to know of the different routes, which in turn may require that the evacuation exits are labelled (such as, exit A, blue exit, floor 1) so as to be distinguishable from each other, and that there is a means of communication of choice of exits or routes.

In some scenarios, communication without alerting attackers will be desirable, perhaps by use of code words, which would need to be included in planning, training and rehearsal.

For chemical biological and radiological incidents consider evacuating uphill and upwind, staying away from the building heating and ventilation systems if the incident has occurred inside a building.

**3.3 Phased evacuation and Partial (zonal) evacuation**

Phased and partial (zonal) evacuation might be decided to give the priority to the people closest to or most at risk from the threat. This approach is similar to that in a fire scenario where typically the floor affected and two floors above are evacuated in advance of other floors.

In crowded places phased or zonal evacuation may be directed in order to control the number of people evacuating so as to not overload internal or external circulation routes, and thereby create further risks arising from moving high density crowds. This is particularly relevant for events and stadia where crowd numbers and densities may be high.

These approaches will normally allow the minimum numbers of people to be evacuated for a given incident and allow the fastest return to normal operations.

**3.4 Invacuation including to protected space(s)**

There are occasions when it is safer to move people away from the threat while remaining inside the venue.

If the threat is outside your venue or the location is unknown, people may be exposed to greater danger if the evacuation route takes them past the threat (such as a suspect device, contaminated environment or attackers). Since glass and other fragments from IEDs may kill or maim at a considerable distance, moving staff inside the crowded place (including to protected spaces) is often safer than evacuating them onto the streets.

© NaCTSO Crown copyright 2017

Invacuation benefits from pre-planning and may benefit from expert advice to help identify safer areas within your building. These locations should be in your plans.

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. However if 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 air, toilet facilities, seating, drinking water, lighting and communications, which are necessary to facilitating staff staying in place for extended periods (perhaps several hours or more). Rehearsal may help validate this.

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.

If instructions are announced via a PA system, avoid naming the specific location(s) (e.g. staircase X) but use code words instead – or the attacker(s) knows where to go.

Go to the CPNI Protected spaces webpage

**3.5 Dynamic Lockdown**

Due to the differences between crowded places in the UK it is not possible to give prescriptive advice on how to lockdown sites or events in response to a fast-moving incident such as a firearms or weapons attack, at the site or in its vicinity. However, this guidance details planning considerations applicable to most sites.

If preventing an attack has not been possible, the ability to frustrate and delay the attacker(s) and reduce the number of potential casualties can be greatly increased through dynamic lockdown.

Advance planning is required to lockdown a site or event and flexibility in those plans may save lives. In order to achieve dynamic lockdown planning should:

- Identify all access and egress points in both public and private areas of the site. Access points may be more than just doors and gates.
- Identify how to quickly and physically secure access/ egress points.
- Identify how to disable lifts without returning them to the ground floor.
- Identify how to stop people leaving or entering the site, and direct people away from danger.
- Identify how your site can be zoned to allow specific areas to be locked down.
- Include staff roles and responsibilities and train staff in these.

Processes need to be flexible enough to cope with and complement evacuation, invacuation and movement to protected spaces.

Dynamic lockdown, especially during the ingress phase of an event may lead to (many) people being 'locked outside' and more vulnerable to the perceived threat. However, allowing continuing ingress might permit the threat to enter the venue and make those inside more vulnerable. Each case must be assessed on the information known at the time and thus good internal and external information and communications systems are crucial. This decision-making process should be considered in staff training and rehearsal.

**3.6 Decision not to evacuate or invacuate**

A decision not to evacuate or invacuate will be reasonable and proportionate if, after an evaluation

© NaCTSO Crown copyright 2017

by the responsible individual, the threat is deemed implausible (e.g. a hoax). In such circumstances police may provide additional advice and guidance relating to other risk management options. It may be considered desirable to ask staff familiar with the venue to check their immediate surroundings to identify anything out of place, making them aware of what to look for including hostile reconnaissance operations.

Do not disregard the possibility that the 'hoax' may have been a test of processes and part of a hostile reconnaissance operation.

Read more about Search planning

## 4. OTHER CONSIDERATIONS

### 4.1 Population of the Crowded Place

It will be helpful to know the population and distribution of people within the crowded places (such as from entry systems) and how this typically changes over time. This influences evacuation times, queuing and delays, space needed for invacuation, and may help the police respond.

### 4.2 Suitability and performance of exit routes

The suitability (e.g. with regards to trip hazards, lighting, pinch-points etc.) and capacities of evacuation routes and exits should be assessed in advance of any emergency. The times to evacuate when one or more exits are unavailable could be helpful in decision-making and should be assessed in advance by calculation, crowd simulation or measurement in an exercise. It will assist with a greater understanding of the timeframes and numbers that can use the exits safely.

Evacuation procedures should also put adequate steps in place to ensure no one else enters the area once an evacuation has been initiated.

### 4.3 Evacuation in non-fire scenarios is not the same as evacuation due to fire

Buildings and events, but not all crowded places, must be designed, maintained and operated to reduce the risk to safety arising from fire. Consequently, staff, contractors and visitors are likely to be familiar with the principles and practice of fire drills including evacuation.

However, the appropriate response to some emergency scenarios may not be to evacuate. Even when the appropriate response is to evacuate then the evacuation response will not necessarily be the same as for a fire scenario. In a fire scenario it will be appropriate to use all available exits. In a terrorism scenario people may be directed to specific exits, which has implications for pre-incident planning.

The use of fire alarms to initiate evacuation should be avoided to reduce the possibility of an incorrect response to an incident. PA systems, if available, provide more flexibility to provide information and instructions appropriate to the scenario and to provide positive confirmation to staff and visitors that the emergency is real, thereby reducing delay in response.

### 4.4 Risks arising from movement in Crowded Places

The sudden movement of large numbers of people creates its own risks. This movement may arise from the fear of a terrorist attack as well as an actual threat. People may be frightened, and the crowd may move in conflicting directions and in a rapid or disorderly fashion.

Research suggests that most people behave rationally in response to the emerging information available to them (which may not be the same or as complete as that available to others) in emergency scenarios, and that rapid and/or disorderly movement away from a changing real or perceived threat is an appropriate response. Rehearsal may help staff, contractors or visitors respond to a threat more effectively (e.g. reduced pre-movement time).

In high crowd densities where there is rapid or disorderly movement, people are more likely to experience a slip, trip or fall, which may in turn lead to trampling or crowd crush, or move into areas presenting hazards such as roads or platform edges. Risks may be exacerbated by poor footway conditions, stairs and escalators. Where stairs are intended to service high crowd flows (such as at stadiums) the stairs are designed with handrails to separate stair channels and with head-of-stair barriers. Some public places that feature high density crowds only occasionally do not have these safety features.

© NaCTSO Crown copyright 2017

Disorderly movement may also increase the risk to more vulnerable members of society such as children, elderly, or people with impairments.

**4.5 Personalised Emergency Evacuation Plans**

Under current fire safety legislation it is the responsibility of the person(s) having responsibility for the building to provide a fire safety risk assessment that includes an emergency evacuation plan for all people likely to be in the premises, including disabled people, and how that plan will be implemented.

The Government guidance on Fire Safety Risk Assessment: means of escape for disabled people provides detailed guidance on how to plan effectively to respond to a fire.

It is sensible to develop personalised plans for disabled staff and visitors for non-fire emergencies requiring evacuation, invacuation or movement to a protected space.

Go to the Government guidance on Fire safety risk assessment: means of escape for disabled people

**4.6 Use of evacuation assembly points and Rendezvous Points (RVP)**

Places of 'relative' safety must be re-assessed prior to and during an incident to ensure they remain so. During planning at least two assembly points in opposing directions should be identified.

The decision to evacuate to an RVP or disperse from the area will depend upon the nature of the threat or attack. Assembly points may not be a credible option where there is an attack. People naturally tend to congregate following an incident; staff training should encompass encouraging people to disperse when appropriate

It is important to appoint people, familiar with evacuation assembly points and RVP, to act as marshals. During an emergency the RVP point should be at least 500 metres from the threat and outside the police cordons. It should not be a car park. You may wish to seek specialist advice from a CTSA or local EPO, who can help to identify suitable assembly points, advise if a location presents any unknown risks, and provide alternative options as part of your planning.

Care should be taken that there are no secondary hazards at the assembly point. It is important to ensure that staff are aware of the locations of assembly point areas for non-fire evacuation as well as those for evacuation due to fire and that the two are not confused by those responsible for directing members of the public to either.

**4.7 Control room response**

There are limitations on the actions control room staff can take in some incidents. Their ability to support public safety will be limited by:

- the degree to which they themselves are at risk
- their own knowledge of the full nature and extent of the incident
- communication channels
- their familiarity with appropriate response options
- the speed at which they are able to recognise, accept and respond to the event
- how psychologically able they are to respond correctly

Consider having alternative off site control room arrangements, perhaps by arranging mutual agreements with other nearby premises where you could establish an emergency control at short notice. The contents of a Crisis Management Kit 'Grab bag' could be stored here.

**4.8 Communications**

**4.8.1 Alerting staff and visitors**

The plan must include a way to alert staff and visitors, including those with disabilities, to evacuate or take other response, and how to report emergencies. Options for communication include:

- Public Address (PA) system. Consider code words for different incidents and dedicated tones/pre-recorded messages to instruct a particular emergency response. Use of PA will need standby power.
- Internal messaging systems: hand held radios, text, email, staff phones, staff alerts/pagers, generic group messaging (e.g. WhatsApp) or organisation-specific apps, 'Pop up' on employees' computers.

© NaCTSO Crown copyright 2017

- Use of Variable Message Signs (VMS) at events or in public spaces.
- Dedicated 'Lockdown' alarm tone.
- Word of mouth.

At some stage an 'all clear' message may be required.

Among the steps managers should take are the following:

- Make sure alarms are distinctive and recognised by all staff as a signal to evacuate the work area or perform responses identified in the plan.
- Stipulate that alarms must be able to be heard, seen, or otherwise perceived by everyone in the workplace. Use tactile devices to alert employees who would not otherwise be able to recognize an audible or visual alarm.
- Consider providing an auxiliary power supply.
- Provide an updated list of key personnel such as the security manager, first aid staff, managers etc. in order of priority, to notify in the event of an emergency.
- Train staff in use of code words. Be aware that the constant use of code words in public areas (e.g. railway stations) are soon recognised by regular users of those spaces (e.g. commuters).
- For multi-occupancy sites, methods of communication from site managers and between all businesses need to be considered.

#### 4.8.2 Informing and updating emergency services

Communication with the emergency services prior to and during the incident is critical. Communication systems should be regularly tested.

#### 4.8.3 Media and Communications

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide details of threats or incidents or the decision-making process relating to emergency response.

## 5. CREATING A RESPONSE PLAN

### 5.1 How do you develop an evacuation policy and procedures?

A disorganised emergency response can result in confusion, injury, and property damage. Therefore, when developing an emergency response plan it is important to determine the following:

- Conditions under which an emergency response would be necessary.
- A clear chain of command and designation of the person(s) in your business authorised to order an evacuation, invacuation or lockdown. There should be an authorised deputy or deputies in the event that the principal responsibility holders are absent for some reason. Those persons must have the actual and perceived authority to instigate an emergency response. The emergency response may have significant safety, personnel and/or financial impact on a business or an event.
- "Evacuation" or "Emergency" wardens to assist others in an emergency and to account for personnel.
- Specific procedures, including routes and exits, and protected areas, if available. Post these procedures and plans where they are easily accessible to all employees.
- Procedures for assisting people with disabilities or who do not speak English.
- Designation of what, if any, critical operations staff will continue or shut down in an emergency. These people must be capable of recognising when to abandon the operation and evacuate/invacuate themselves.
- A system for accounting for personnel following an emergency.
- Consider employees' transportation needs for community-wide evacuations.

### 5.2 Key personnel in managing an emergency response

The Board of Directors managing the crowded place will have identified the Security Manager or designated an individual as responsible for making decisions in an emergency; key responsibilities will be:

- Assessing the situation to determine whether an emergency exists requiring activation of emergency procedures.
- Supervising all efforts.

© NaCTSO Crown copyright 2017

- Coordinating outside emergency services and other relevant responders, and ensuring that they are informed when necessary.
- Directing the shutdown of site/plant operations when required.

It is critical that staff know who the coordinator is and understand that person has the authority to make decisions during emergencies.

In addition to a coordinator, emergency or evacuation wardens may be designated to help move employees from danger to safer areas during an emergency. Moving groups or crowds is more effective when crowds are 'pulled' to an exit rather than 'pushed', so consider training wardens to activate the evacuation by leading others towards the safest routes rather than telling them where to go.

Employees designated to assist in emergency evacuation procedures should be trained in the complete workplace layout and various alternative escape routes. All employees and those designated to assist in emergencies should be made aware of employees with special needs who may require extra assistance, how to use the buddy system, and hazardous areas to avoid during an emergency evacuation.

**5.3 What role should staff play in developing an emergency plan?**

The best emergency plans include the management team and employees in the planning process. Explain the goal of protecting lives, property and assets in an emergency, and encourage staff to offer suggestions about potential hazards, worst-case scenarios, and emergency responses.

After developing the plan, review it with staff to ensure everyone knows what to do before, during and after an emergency, and make sure that employees receive proper training for emergencies, including rehearsal and exercises. Staff commitment and support are critical to the plan's success. Keep a copy of your emergency response plan in a convenient location where employees can get to it, or provide all employees a copy. Research shows that pre-warning staff through such sessions does not elicit responses of fear and panic, and that well informed individuals react better.

**5.4 Under what conditions should you call for an evacuation?**

The responsible person within the organisation managing the crowded place should be responsible for making the decision to evacuate, invacuate, lock down, shut down, or continue operations. Protecting the health and safety of everyone in the crowded place should be the first priority.

In an emergency, the police or fire and rescue service may require you to evacuate your premises. In some cases, they may instruct you to shut off the water, gas, and electricity. If you have access to radio, television, or other media listen to newscasts to keep informed and follow whatever official orders you receive.

The type of crowded place or building you work in may be a factor in your decision. Most buildings are vulnerable to some of the effects of explosions. The extent and nature of the damage depends on the type of incident and the building's construction. Some buildings will collapse and others will be left with weakened floors and walls. Internal walls can provide some 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. When making changes to convert a space to open plan accommodation, try to ensure that there is no significant reduction in staff protection, for instance by improving glazing protection.

**5.5 How do you establish evacuation routes and exits?**

When preparing an emergency response plan, designate primary and secondary evacuation routes and exits. To the extent possible, ensure that evacuation routes and emergency exits meet the following conditions:

- clearly signed and well lit – floors, stairwells, exits, gangways
- unobstructed and clear of debris at all times. Regularly check outside exit doors to ensure they have not been blocked by others
- wide enough with sufficient capacity to accommodate the number of evacuating personnel

© NaCTSO Crown copyright 2017

- unlikely to expose evacuating personnel to additional threats (including crowd safety risks along the route itself)
- if you prepare drawings that show evacuation routes and exits, post them prominently for all employees to see but keep building plans out of the public sphere

Where emergency services notify of transport system having been shut down, contemplate sharing this information with staff before telling them to disperse towards a certain areas.

**5.6 Coordinating Efforts**

There is no specific requirement to do so, but it may be useful to coordinate efforts with other companies or groups nearby to support the effectiveness of the plan. In addition if you rely on assistance from local emergency responders such as the FRS, or other outside responders, you may find it useful to coordinate emergency plans with these organisations. This ensures that you are aware of the capabilities and plans of these outside responders and that they know what you expect of them. Additionally, it may be helpful to know how and where your neighbour is planning to evacuate to, especially if streets are narrow and building populations are high.

**5.7 What employee information should your plan include?**

In the event of an emergency, it could be important to have ready access to important personal information about your employees. This includes their home telephone numbers, the names and telephone numbers of their next of kin, and medical information.

**5.8 What type of training do your employees need?**

Educate your employees about the types of emergencies that may occur and train them in the proper course of response. Be sure all your employees understand the function and elements of your emergency plan, including types of potential terrorist attack methodologies, reporting procedures, alarm systems, evacuation plans, and shutdown procedures. Identify hazards you may have onsite such as flammable materials, toxic chemicals, radioactive sources, or water-reactive substances.

**5.8.1 General training for your employees should address the following:**

- individual roles and responsibilities
- threats, hazards, and protective responses – Project Griffin and Project Argus
- notification, warning, and communications procedures
- emergency response procedures
- evacuation, shelter, and accountability procedures including different threats may need different responses
- location and use of common emergency equipment
- emergency lockdown procedures
- you also may wish to train your employees in first-aid procedures

Once you have reviewed your emergency response plan with your employees and everyone has had the proper training, hold rehearsals as often as necessary to keep employees prepared. Include outside organisations such as police, fire and rescue, ambulance service and partners. After each exercise, gather management and employees to evaluate the effectiveness of the drill and work to improve it.

**5.8.2 How often do you need to train your employees?**

Review your plan with all your employees and consider requiring annual training in the plan. Also offer training when you do the following:

- develop your initial plan
- hire new employees, take on new contractors
- introduce new equipment, materials, or processes into the workplace that affect evacuation routes
- change the layout or design of the facility
- revise or update your emergency procedures
- there is  change in threat or vulnerability

© NaCTSO Crown copyright 2017

**5.9 How can you assist your employees after an incident?**

Accounting for all employees following an evacuation is critical. Confusion in the assembly areas can lead to delays in rescuing anyone trapped in the building or venue, or unnecessary and dangerous search-and-rescue operations. To ensure the fastest, most accurate accounting for staff, you may want to consider including these steps in your emergency plan:

- Designate assembly points where employees should gather after evacuating when this is safe to do so; dispersal should be an alternative.
- Take a headcount after the evacuation. Identify the names and last known locations of anyone not accounted for and pass them to the official in charge (with a large company, managers should be accountable for their teams) consider the use of off site T cards (personnel booking in and out cards) at sites to identify who was on site and off site.
- Establish a method for accounting for non-employees such as suppliers and customers.
- Establish procedures for further evacuation in case the incident expands. This may consist of sending employees home by normal means or providing them with transportation to an offsite location.

**5.9.1 What medical assistance should you provide during an emergency?**

Check if your company has formal first aid training. There are a number of online apps available to support staff should they be required to give first aid after an attack. Citizen Aid, Red Cross and St Johns Ambulance for example.

**5.10 At a minimum, your emergency plan must include the following:**

- evacuation procedures and route assignments, such as floor plans, workplace maps, and protected/safe or refuge areas
- names, titles, departments, and telephone numbers of individuals both within and outside your company to contact for additional information or explanation of duties and responsibilities under the emergency plan
- identified personnel who will 'lead' in the evacuation to draw people to safe exits
- procedures for employees who remain to perform or shut down critical operations, or perform other essential services that cannot be shut down for every emergency alarm before evacuating
- first aid responsibilities
- procedures to account for all employees after an evacuation
- the site of an alternative communications centre to be used in the event of an attack or incident
- a secure on/off-site location to store originals or duplicate copies of accounting records, legal documents, your employees' emergency contact lists, and other essential records
- a crisis response kit 'grab bag'
- consider designating an assembly location

You may want to complete the Crisis response kits checklist

**GO TO SECTION CONTENTS**

Go to the Government Emergency response and recovery webpage

Go to Glossary

© NaCTSO Crown copyright 2017

## APPENDIX A: EMERGENCY RESPONSE PLANNING – ORGANISATIONS

**1. Plan – pre-incident**

Think ahead

a. Consider threats, vulnerabilities and assess the risks.

b. Develop a plan (Emergency response plan).

c. Security manager to plan for evacuation or invacuation; identify protected spaces .

d. Identify individuals' roles and responsibilities (e.g. security manager, personal evacuation plans for disabled individuals etc.).

e. Provide relevant guidance and information to staff, contractors and visitors.

f. Prepare your personnel and contractors through training and rehearsal.

g. Identify critical operations/function.

h. Identify protected spaces.

i. Develop pre-scripted messaging/alerts how you will communicate with staff, visitors etc.

j. Plan how you will deny, detect deter hostile reconnaissance.

k. Plan how you will deny, detect, deter and delay attacks or threats to protect your most valuable assets (physical and personnel measures).

l. Ensure infrastructure; signage, lighting, floor levels, lifts, stairs are clearly marked and labelled, CCTV is functional to facilitate an evacuation/invacuation.

m. Prepare floor plans.

n. Establish if your control room is capable of being operationally effective against different attack types and can it be secured/defended.

o. Establish RVPs (assembly points) if appropriate for incidents.

p. Regularly check systems and equipment.

q. Prepare crisis response kits (incl. personal information about your employees).

r. Establish working relationships with neighbours.

s. Prepare checklists to support responders.

t. Ensure staff have adequate first aid training.

Remember: Plans must be event and location specific

**2a. Incident – evaluate**

**Consider your options and use your judgement**

a. Stay calm.

b. Gather information.

c. Assess the situation, determine the type of incident, location(s), attackers, hazards, weapon. Do not wait for police.

d. Implement plans.

e. Establish where is the safest place or if any response is required. Is it safe to evacuate? Are there other attackers, devices, obstructions, fires etc.?

f. Establish the safest route(s) to leave.

g. Consider:
   1. Full site evacuation
   2. Staged/zonal/partial/directional evacuation or invacuation
   3. Internal/inward invacuation to protected space/area
   4. Lockdown
   5. Decision to take no response

h. Do any critical operations require protecting or shutting down?

i. Can I stop other people entering the site?

j. Determine if a search of the site is required.

k. Monitor news and media channels.

l. Communicate with partners.

There is a danger you may be overwhelmed with information. Determine how to gather and transfer information in a controlled manner to support an effective response.

© NaCTSO Crown copyright 2017

**2b. Incident – respond**

**Take responsibility**

Leadership is key, make a dynamic risk assessment and take action. Decisive individuals will save lives.

a. Communicate: let staff and people know what's happening and where possible advise as to the most appropriate response.

b. CALL 999 – Follow the RUN HIDE TELL principles if appropriate.

c. Make contact with the emergency services and update and support them.

d. Continue to monitor progress of attackers using assets e.g. CCTV.

e. Prevent people from entering the venue if it is not safe to do so.

**3. Post incident**

**Recovery**

a. Account for all individuals.

b. Determine a method for notifying families of individuals affected.

c. Assess the psychological state of individuals at the scene. Seek professional guidance.

d. Consider processes for further emergency response in case the incident expands.

e. Record your responses.

f. Determine if a search of the site is required.

g. Identify and fill critical personnel and organisational gaps.

h. Use lessons learned to train and rehearse staff.

Read more about Business continuity

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

## APPENDIX B: INDIVIDUALS – PERSONAL SAFETY

**1. Plan – pre-incident**

**Think ahead**

a. What are your plans if there were an incident?

b. Be aware of your surroundings including evacuation routes (events and building).

c. Note the locations of exits.

d. Identify areas where you could take cover (Hide/cover from view).

e. Ensure you have contact details of important individuals e.g. family.

f. Understand what to do for building alarms.

g. Consider sometimes using different entrances into work so you are more familiar with alternatives for evacuation.

**2a. Incident – evaluate**

**Consider your options**

a. Stay calm.

b. Assess the situation as quickly as possible and consider your options.

c. Where possible identify where you are in relation to the incident.

d. Establish where is the safest place.

e. Listen to instruction communicated by those in authority.

f. Your options will be:

1. Evacuate and get yourself and others to safety, possibly via safe routes. RUN.
2. Remain where you are and await further information.
3. Go to a protected area/shelter.
4. HIDE.

**2b. Incident – respond**

**Take responsibility**

Leadership is key, make a dynamic risk assessment and take response. Decisive individuals will save lives.

a. Evacuate in a safe and orderly manner where possible.

b. Identify the safest route.

c. Assist others if it is safe to do so.

d. Go to RVPs/assembly points if appropriate.

e. TELL police when it is safe to do so.

## 3. POST INCIDENT

**Recovery**

a. If you have witness and attack, report what you saw. Make yourself known to police. Any photographs or video footage should be passed on to the police.

b. If you are a victim of an attack, contact the police.

c. Contact family and friends to let them know you are safe.

Remember: Follow the RUN, TELL, HIDE principles

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

**Planning considerations for each attack type to support an evacuation/invacuation/lockdown**

# Appendix C: Attack type

Click on an attack type to read the factors for consideration when planning or instigating an evacuation, invacuation to a protected space or lockdown. Actions should be reasonable, necessary and proportionate based upon the risk.

FIREARMS AND WEAPONS ATTACK

VEHICLE AS A WEAPON

PBIED

IED

VBIED - NON PEN

VBIED - PENETRATIVE

BOMB THREAT

CBRN

UVIED

POSTAL IED

© NaCTSO Crown copyright 2017

## MANAGING RISK

- Have you conducted a risk assessment?
- Has an individual been appointed who is responsible for security?
- Have you an Emergency Response Plan?
- Under what circumstances would you instigate an evacuation/ invacuation/lockdown?
- Have you establish the safest evacuation routes and protected spaces?

## PHYSICAL SECURITY FACTORS

**Critical points**

- Are there critical areas of the site that need to be shut down or are vulnerable?
- Can you lockdown the site?

**Crowd density and building occupancy**

- Can the entrances, exits, routes and protected spaces accommodate numbers?
- Are your exits ever inadvertently blocked e.g. during loading or stock up?
- Can you prevent other people entering?

**Factors that affect the suitability of egress routes may include:**

- Stairs/escalators
- Lifts
- Exits (direction of open)
- Seating and gangways
- Signage to identify exits and routes
- Widths and capacities/pinch points and obstructions/distances/slip/ trip/fall
- Evacuation timeframes
- Volume of staff/visitors
- Have you identified obstructions to an evacuation or invacuation?

**Building structure**

- Have you identified what risks or protection the building structure presents e.g. glazing, steel frame, brick work offer against different attack types

**Access control**

- Will this prevent escape or protect staff?

**Lighting**

- Is this suitable to support an invacuation or evacuation?

**Control rooms**

- Are they protected from diffent attack types?

**Alarms**

- Do you have alarms to alert staff and public?

**CCTV**

- What does it cover, is it monitored, can it track an attack?

**Hazards**

- Have you removed items and hazards that may assist a terrorist attack? (fuel, scaffolding poles etc.)

i Read more about Good housekeeping

**Electrical supply**

- Do you require backup generators?
- Is the electrical supply protected?

## PERSONNEL SECURITY FACTORS

**Threat awareness**

- Have staff been briefed on threats and methodologies?

**Training and rehearsal exercising**

- Have you conducted rehearsal exercises to validate learning?
- When did you last rehearse?
- When did you last train your staff? e.g. first aid, evacuation
- Do staff know where are the safe places, routes, assembly points and exits?
- Can staff recognise suspicious behaviour?
- Can staff respond effectively to suspicious items?

**Role and Responsibility**

- Do staff understand their key roles?
- What is the role of coordinators and evacuation marshals during an emergency?
- Have you identified what equipment you should provide for emergencies?
- Do you have plans for vulnerable and disabled staff and visitors?

## COMMUNICATION

- Are communication networks effective?

**Alerts and messaging**

- What alerts, alarms, coded and or pre-scripted messaging have you prepared?
- How do you alert employees and visitors to an emergency?

© NaCTSO Crown copyright 2017

**Command and Control**

- How will you communicate: radio, PA/VA, mobile phone, social media?
- Are you able to contact other sites and partners?
- Can you stop others entering?
- Who will inform the emergency services?
- Can staff communicate directly with and assist the emergency services?
- Have you a media strategy?

## RECOVERY

- Have you a Business Continuity Plan?
- How to account for employees after an evacuation?
- Do you know who your critical staff are?

GO TO SECTION CONTENTS

Consider another Attack type

Go to Glossary

© NaCTSO Crown copyright 2017

# CCTV

## 1. INTRODUCTION

This guide provides protective security advice, with a specific focus on CCTV or video surveillance systems, for those responsible for security of crowded places and small and medium enterprises (SMEs). All sites are different and it is not possible to give prescriptive advice as each site has its own unique characteristics.

## 2. CCTV GUIDANCE AND OPERATION

CCTV or video surveillance systems, designed for both large crowded places and small and medium enterprises (SMEs) can play an important role in the early identification of crime and critical incidents, as well as the health and safety of staff and end users, whilst assisting in the control of access and public liability claims.

Your CCTV system could be effective for post incident evidence gathering and forensic analysis or to quickly identify offenders or other suspicious behaviour.

If you monitor or regularly review your recorded images this may identify suspicious activity or terrorist attack planning (terrorist attacks may be preceded by a period of planning against your site, we call this 'hostile reconnaissance') but only if your cameras are positioned in the right place and have clear images. Following the initial detection of an intrusion or incident, CCTV systems can be monitored by your staff to assist in tracking offenders, monitoring of a situation and could provide vital information that will aid the emergency services.

## 3. CAN WE IMPROVE THE EFFICIENCY AND EFFECTIVENESS OF VIDEO SURVEILLANCE IN A COUNTER-TERRORISM ROLE?

An Operational Requirement (OR) allows you to identify the need and the intended purpose of a CCTV system, which will drive its design and the parameters for operation. This will ensure the system is flexible and future-proofed and is appropriate for your specific needs and address:

1. the purpose of your CCTV system.
2. why do you need cameras and what information is needed from each camera in that specific location?
3. the level of detail you require for each camera, how will you store images and for how long?

An OR process helps organisations invest wisely in security measures, enabling them to implement an integrated approach to security and identify security measures which are proportionate to the risks they face. A lot of information is going to be retrospective and reviewed post incident, therefore the design of the system is important to get the correct detail and quality.

Go to the CPNI Operational Requirements webpage

## 4. PLANNING NEW OR AUDITING EXISTING SECURITY PROJECTS

There are some fundamental stages when planning new or auditing existing security projects:

- understand and identify the security risks that your organisation faces
- consider the nature of hostile reconnaissance, where it may be conducted at your site, and what you can do to deter or detect it
- develop an OR statement of need for each camera in each location
- the OR will enable you to design your CCTV system and consider the various types of CCTV surveillance technologies available on the market
- carry out an audit of your cameras against your operational requirement

By completing this process you assess, develop, and justify the investments you need to make to protect your critical assets against security threats. The OR will determine the technical design of the CCTV system to have effective detection capabilities focussed in the right areas to help deter, disrupt or detect hostile reconnaissance and criminal activity.

© NaCTSO Crown copyright 2017

## 5. CCTV SYSTEM – TECHNICAL DESIGN

Even newly installed CCTV systems can be designed badly and the police have often found that there has not been adequate consideration given at the OR stage. The Home Office Centre for Applied Science and Technology (CAST) and the NPCC have published many useful guidance documents relating to CCTV that can assist security managers with the design of their system.

Using these guides will enable you to work alongside your CCTV contractor to get a system that is fit for purpose and the needs your organisation.

Go to the Government CCTV guidance webpage

Go to the CPNI CCTV guidance webpage

### 5.1 Factors to consider

When choosing the best location for your cameras and the number and type of CCTV camera and lens it is important to consider the view on the monitor, the distance from the target, the angle of view, the lighting conditions and the prevailing weather. Each of these factors will impact on the live and recorded image quality and if not considered with particular attention to your OR, the system may not meet your needs.

Modern cameras produce images and have superior colour to that of previous systems, meaning that they are even more effective at capturing important details over a larger field of view. With a greater resolution, significantly more data is being captured by a camera than before, so compression technology may be used and the storage requirements could be significantly increased. If the recording process has utilised image compression technology it could result in a reduction in picture quality compared to the live view and this may affect the quality of the recorded image and the number of days' retention to allow for evidential recovery.

The movement from traditional analogue surveillance technology to IP (digital) surveillance solutions has given security professionals access to a much broader functionality. Video analytic software is now affordable to SMEs. Video analytics can provide a host of features allowing operators to do more with surveillance footage and quickly identify and track suspects. CCTV software can serve particular security applications, such as traffic monitoring, car parking control and enforcement, which can link with Automatic Number Plate Recognition (ANPR).

### 5.2 Selecting a reputable and diligent contractor

When selecting a CCTV installer, check they are registered with a UKAS accredited inspectorate. This will ensure they operate to the highest level of business excellence, comply with the relevant British and European (BS and EN) Standards and work to an approved code of practice for the design, installation and maintenance of systems.

An approved, reputable and diligent contractor will provide a technical specification for the system and should perform an audit and commissioning test of the system to prove, to you as the end user, that the system meets your operational requirement and your design criteria.

Image quality can be measured against the Rotakin® standard. The Rotakin® target was developed by CAST as a means of auditing the efficiency of a CCTV system.

Go to the CAST resources for the crime prevention industry webpage

### 5.3 Will my system allow the prosecution of offenders?

CCTV camera evidence can be compelling, though issues of image quality are a factor if CCTV images are used for court. The operational requirement and technical design would consider the nature of the activity to be observed. The purpose of the observation can be:

- identification, matching a face to a database
- recognition, differentiating between objects within a scene
- observing, some characteristic details of the individual, whilst the view remains sufficiently wide to allow activity surrounding an incident to be monitored
- detection of an object within the scene

The access points to a site may provide the best opportunity to obtain the identification of individuals or

© NaCTSO Crown copyright 2017

vehicles as they enter or exit the site or other areas that are critical to the safe management and security of your operation.

If recorded images may be seized by police and used as evidence you need to consider the continuity of evidence.

Your recording equipment should be placed in a secure area with restricted access. The system should have sufficient storage capacity for 31 days good quality pictures. If downloaded, all recordings on discs should be kept in a secure place.

If an incident occurs the images should be copied onto a CD-R. A record should be kept of movement of the CDs showing a number, times, dates and names of those handling the CD. All used CDs should be destroyed and disposed of securely.

**5.4 Is your CCTV system legally compliant?**

If CCTV is an existing element within your security and management strategy, make sure that you have a CCTV policy describing how it is managed in compliance with the Data Protection Act 1998. If you contract in surveillance CCTV operators, they must be licensed by the Security Industry Authority (SIA).

Go to the Data Protection Act CCTV guidance webpage

Go to the SIA Licensing CCTV webpage

## 6. INCIDENT RESPONSE

Not all crowded places and SMEs will have an efficient, functioning, well-sited CCTV system with trained operators proactively looking for suspicious activity, to direct security officers or police on the ground. So consider:

- If there is an increase in threat level to your location can staff be deployed to actively monitor your CCTV system?
- If you monitor or regularly review your recorded images this may identify suspicious activity or terrorist attack planning. Do you record and report any suspicious activity, that you think may constitute hostile reconnaissance, to the police?
- If you become aware of an incident; how fast is your response time to enable staff to monitor and review your CCTV?

The number of terrorist incidents in Europe and elsewhere has underlined the importance of our emergency response, both to relatively unsophisticated attacks by lone individuals, to much more complex attacks, particularly involving firearms and explosives at multiple locations.

## 7. TRAINING

While CCTV, thermal imagers or video analytics are useful technology, all these will rely to some extent on the effectiveness of the control room and the security staff. Project Griffin (a national police initiative) is specifically designed for front of house staff and security, to raise awareness of counter-terrorism.

Go to the Project Griffin - Industry Self-Delivery webpage

## REFERENCES AND LINKS

Home Office CCTV guidance documents offer information including:

- guidance for users wishing to buy a CCTV system that is fit for purpose
- procedures and guidance retrieving video and image evidence from digital CCTV systems
- guidance on the processes involved in the handling of digital images
- UK police requirements for digital CCTV systems

© NaCTSO Crown copyright 2017

**GO TO SECTION CONTENTS**

Go to the CAST CCTV guidance webpage

Go to the CAST resources webpage

Go to the CPNI CCTV Guidance

Go to the CPNI intruder detection, tracking, monitoring and lighting webpage

Go to the CPNI Operational Requirements webpage

Go to the Data Protection Act CCTV Guidance for organisations

Go to the Data Protection Act CCTV Guidance for the public

Go to the NaCTSO website

Go to the Surveillance camera commissioner website

Go to Glossary

© NaCTSO Crown copyright 2017

# Access control

## 1. INTRODUCTION

It is important to ensure that your site is kept secure, whilst remaining accessible to your visitors or customers. There will be areas within your site or venue that, for various reasons, should be kept closed to the public. There should be clear demarcation between your public and private areas, with appropriate access control measures in place. Measures at crowded places will differ depending upon the conditions of entry. To be effective, any system requires active management and appropriately trained staff.

## 2. APPEARANCE

Your access control system is a strong indicator of the security regime at your site and should be complimented with clear signage. A challenge culture by staff will also deter hostile reconnaissance. However, consider balancing the deterrent effect of appropriate signage with the possible assistance being given to an adversary carrying out hostile reconnaissance.

Go to the CPNI Control of access webpage

## 3. OPERATIONAL REQUIREMENTS

When installing a new access control system, you should specify your Operational Requirement (OR). A Level 1 OR (OR1) will identify the problem you are trying to solve and the most appropriate solution.

Go to the CPNI Operational Requirements webpage

## 4. EASE OF ACCESS

Examine the layout of your access control system. Ensure that your entry and exit procedures allow legitimate users to pass without undue effort and delay. You should consider how your access control system will work in busy areas at peak times. Access measures should be appropriate for the site and not unnecessarily onerous.

## 5. POLICY AND PROCEDURE

You should have clear policies and procedures for how the access control system will be used and operated. You should consider how misuse of the system by staff, visitors and customers will be challenged. Staff should feel empowered to challenge anyone entering an area without the correct pass or who looks in any way suspicious.

## 6. TRAINING

Ensure your staff are aware of the role and operation of your access control system. If you have any access control equipment in place your installer should provide adequate training. Training should include the action to take:

- if a pass is lost
- if a person needs to be challenged
- in response to suspicions behaviour

## 7. SECURITY CULTURE

An effective access control system should incorporate adequate training of staff, and should highlight how to overcome bad practice such as tailgating and holding doors open, coupled with the promotion of a good security culture. Staff should feel safe to challenge or report suspicions.

## 8. SYSTEM MAINTENANCE

Your system should be maintained and kept in good working order. Your installer should supply all relevant system documentation e.g. log books and service schedules. Be aware of the actions required in the event of a system failure. These failures must be dealt with immediately and a contingency plan put into place. This may be to secure a door, or provide a security officer at the point of failure, with all actions being recorded. You should ensure that you have a suitable maintenance agreement in place which will rectify problems quickly.

## 9. MANUAL ACCESS CONTROL

If after carrying out the OR1 you decide that a manual locking system is appropriate, there should be a robust management process in place incorporating:

### 9.1 Key management

Key management is crucial in order to maintain the integrity of the system. You should keep a record of all keys issued and conduct regular audits. If a key cannot be

© NaCTSO Crown copyright 2017

accounted for, there should be a contingency plan to deal with a potential compromise of access control.

**9.2 Additional management control systems**

An electronic lock may be appropriate. This offers a 'halfway house' between mechanical locks and a fully electronic access control system. If mechanical PIN code locks are used you should have a plan in place to change PIN codes regularly. Best practice is to change them after a member of staff leaves, after a security breach or every 6 months.

## 10. INTEGRATION

Your access control system should support other security measures. Consider system compatibility between access control, alarms, CCTV and text alert systems.

## 11. COMPLIANCE

Your access control system should be compliant with:

- The Equality Act 2010
- The Human Rights Act 1998
- Health and Safety at Work Act 1974
- The Data Protection Act 1998
- The Regulatory Reform (Fire Safety) Order 2005
- The Fire (Scotland) Act 2005

Your access control system will have a set response to fire alarms i.e. doors automatically unlock when an alarm sounds. For your critical areas such as control rooms, it must be remembered that fail-safe systems must be compliant with both health and safety and security requirements. Ensure that when you specify an access control system, you consider what areas may remain locked in an emergency, as security should never compromise safety.

## 12. LOCKDOWN PROCEDURES

Due to the potential for Firearms and Weapons Attacks and protest activity for example, it is important for you to consider implementing a dynamic lockdown procedure. You should consider how your access control system aids or hinders your lockdown procedures. There may be features in your access control system that can be utilised during a lockdown. These features should be quick and simple to activate and staff should be trained in their operation.

Read more about Evacuation, invacuation, lockdown, protected spaces

## 13. VETTING PROCEDURES

You should consider how vetting procedures impact on access control. You will need to decide if staff have access to all areas, or if there are restricted areas to your site. Staff and visitors should only be given access to the areas required for their role. Passes may vary in type, dependent upon the area accessed.

The manager of the access control system has a critical role and should be appointed accordingly. Only this person or their deputy should issue passes. Passes must be signed for once the identity of the recipient has been confirmed. Out of hours, the security supervisor may be authorised to issue temporary passes but this will be extremely rare and any visitor out of hours should be escorted. Any passes issued out of hours must be of limited duration.

## 14.SEARCH PROCEDURES

If y our OR identified that searching is necessary at your site, then there are a number of considerations. The primary one relates to the nature of the threat you face. You must identify the aim of the search and the type of items you are searching for. You should use appropriately trained staff, use well maintained equipment and have sufficient space and a suitable environment to conduct the search.

Read more about Search planning

**14.1 Training**

Effective searching requires suitably trained staff who know what to look for, how to search and the action to take if anything is found. BSI PAS 127:2014 Checkpoint

© NaCTSO Crown copyright 2017

Security Screening of People and their Belongings: Guide. This guide aims to provide comprehensive guidance to security managers and contractors on the specification, design and delivery of checkpoint screening processes.

PAS 127:2014 may be purchased from BSi.

Go to the CPNI Screening people and their belongings webpage

Go to the CPNI Screening vehicles webpage

Go to BSI PAS 127:2014

## 15. VEHICLE PROCEDURES

If your OR identifies the need for vehicular access control then there are a number of considerations. Search procedures must be consistent with the threat. The ideal solution is to restrict the number of vehicles accessing your site and any search should be conducted as far away as is reasonably practicable. Ideally, access will be afforded only to vehicles that are booked in and expected, with the identity of the occupants confirmed.

### 15.1 Vehicle access passes

Certain vehicles may need to routinely access your site. It may be prudent to issue vehicle passes to identify vehicles and the management of these passes should be commensurate with all the other access control measures in place. Vehicles that need to gain access without a pass should only be with prior arrangement.

### 15.2 ANPR

Automatic Number Plate Recognition (ANPR) may be a useful addition to an integrated security regime, but will only provide information related to a registration plate and should not be relied upon alone.

## 16. INCREASED THREAT

At times of increased threat it may require further access control measures, which may be for staff, vehicles or both. This should be reflected in the site security plan. Vehicle access control may be enhanced by the application of Hostile Vehicle Mitigation (HVM).

Read more about Threat level and building response plans

## 17. SUMMARY

The OR process is fundamental to planning an efficient security solution and access control is no exception. Be it controlling pedestrian access to certain areas or vehicles into a site, the principles are the same.

Know who or what is allowed to go where and allocate passes to reflect this, with access suitably limited. Any access control system is only as good as the procedures and the people that govern its use and a good security culture is paramount in ensuring your site remains secure.

**GO TO SECTION CONTENTS**

You may also want to complete the Access Control Checklist

Go to the CPNI Access control and locks webpage

Go to Glossary

© NaCTSO Crown copyright 2017

# Search planning

## 1. INTRODUCTION

The regularity and scale of searches should reflect the threat and be proportionate to the risks faced by the particular organisation and site. Searches of your site or event can be conducted as part of your daily good housekeeping routine. They should also be conducted in response to a specific threat (such as breach in perimeter security, or a bomb threat) and when there is a heightened response level. It is recognised, that for the majority of venues or events the responsibility for the implementation of any search planning following a risk assessment will fall upon the security manager.

The following advice is generic for most sites and events, but recognises that they often operate differently. If considered necessary, advice and guidance on searching should be available through your local Police CTSA, Police Search Adviser (POLSA) or Police Security Coordinator (SECCO).

## 2. SEARCH PLANS

Search plans should be prepared in advance and staff should be familiar and trained in them:

- The conduct of searches will depend on local circumstances and knowledge, but the overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to invacuate or evacuate your venue or event in response to an incident or threat, you will also need to search prior to re-occupancy to ensure it is safe.
- The member(s) of staff nominated to carry out the search do not need to have expertise in explosives or other types of device. They must be familiar with the place they are searching and what they are looking for. This may include items that are hidden, obviously suspicious or not typical of that environment. Staff must be aware of the appropriate response when finding suspicious items.
- Ideally searches should be conducted in pairs; to ensure searching is systematic and thorough.

## 3. SEARCH PLANNING

Consider dividing your site or venue into sectors for searching. If the site is organised into departments and sections, these should be identified as separate search sectors. Each sector must be of manageable size. Remember to include the following areas in your search plan: stairs, fire escapes, corridors, toilets, lifts, car parks, service areas, boiler houses and other areas outside that are within your perimeter.

Each sector search plan should have a written checklist, signed when completed for the information of the Security Manager.

If evacuation is considered or implemented, then a search of the assembly areas, the routes to them and the surrounding area should also be considered where possible. Staff should be encouraged to be particularly vigilant during invacuations and evacuations.

Test and exercise your search plan regularly. The searchers need to get a feel for the logical progression through their designated area or sector and the length of time this will take. They also need to be able to search without unduly alarming any visitors. You should review your search and act on any lessons learnt.

### 3.1 Initiating searches

Consider the most effective method of initiating searches especially those that are non-routine. You could:

- send a message to the designated search teams over a public address system (the messages should be coded to avoid unnecessary disruption and alarm)
- use personal radios, pagers or mobile phones

### 3.2 Actions on discovery of suspicious items

Ensure the searchers know what to do if they discover a suspicious item. Action will depend on the nature of the item and the location; the general principals are Confirm, Clear, Communicate and Control.

Do not touch or move suspicious items. Where there is a control room consider using CCTV to identify those that

© NaCTSO Crown copyright 2017

have left the items in suspicious circumstances. Keep police informed of your actions.

Read more about Suspicious items

**3.3 Search and screening people and their belongings**

Screening people and their belongings at entry points can help reduce the likelihood of explosive devices, weapons, and other hazardous or prohibited items being brought into a site.

- ensure search and screening regimes in place are professional
- ensure search and screening regimes are designed to address the detection priorities of your site
- ensure that any search and screening measures are effective and conducted in accordance with documented policies and procedures
- consider provisional search and screening on the approach or outside the venue, for example a visual check inside jackets and bags
- provide effective public address messaging to people as they approach, asking people to prepare for additional search and screening, this should reduce unacceptable delay
- prior notification (at point of sale or media) of these extra security measures and encouraging people to arrive early, will smooth peaks and allow safe and effective searching
- ensure the search area has sufficient space and protection from the elements
- ensure you have properly briefed staff conducting searches, on what they are searching for, their powers, what to do if they find a prohibited or suspicious item

Go to the CPNI Screening people and their belongings webpage

Go to the CPNI Screening vehicles webpage

Go to BSI PAS 127:2014

## 4. APPLICATIONS

Search and screening measures are most easily implemented on entry to secure sites and buildings, they offer preventative and deterrent benefits, and will typically focus on:

- screening people and their belongings
- screening vehicles
- screening mail and courier deliveries
- screening bulk deliveries
- searching buildings and surrounding areas

You may also want to complete the Good housekeeping checklist

Read more about Mail handling

Go to the CPNI search and screenings webpage

Go to BSI PAS 127:2014

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Mail handling

## 1. INTRODUCTION

### 1.1 Small deliveries by courier and mail handling

Most businesses will receive a large amount of mail and other deliveries and this offers a potentially attractive route into premises for terrorists.

Go to PAS 97: 2015 Mail screening and security specification

PAS 97 is aimed at assisting organisations in assessing the risks they face from postal threats, and implementing appropriate screening and security measures.

### 1.2 Delivered Items

Delivered items, which include malicious letters, parcels, packages and anything delivered by post or courier, have been a commonly used tactic by criminals and terrorists. 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.

Delivered items may be explosive, incendiary or contain sharps or blades, or chemical, biological or radiological (CBR) material. The phrase 'white powders' is often used in the context of mail and encompasses CBR material as well as benign materials (note: such materials may not be white and may not be powders). Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.

A delivered item may have received some rough handling in the post and so is unlikely to detonate through being moved. Any attempt at opening it, may set it off or release the contents. Threat items come in a variety of shapes and sizes; a well-made device will look innocuous but there may be tell-tale signs.

## 2. INDICATORS

### 2.1 Indicators to Suspicious Deliveries/Mail

General indicators that a delivered item may be of concern include:

- unexpected item, especially if hand delivered
- a padded envelope ('Jiffy Bag') or other bulky package
- additional inner envelope or other contents that may be difficult to remove
- labelling or excessive sealing that encourages opening at a particular end or in a particular way
- oddly shaped or lopsided
- envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- marked 'to be opened only by...' 'personal' or 'confidential'
- item addressed to the organisation or a title (rather than a specific individual)
- unexpected or unusual origin (postmark and/or return address)
- no return address or return address that cannot be verified
- poorly or inaccurately addressed, address printed unevenly or unusually
- unfamiliar writing or unusual style
- unusual postmark or no postmark
- more stamps than needed for size or weight of package
- greasy or oily stains emanating from package
- odours emanating from package

### 2.2 Explosive or incendiary indicators

Additional explosive or incendiary indictors include:

- unusually heavy or uneven weight distribution
- small hole(s) in envelope or wrapping

### 2.3 'White powder' indicators

Additional White powder indictors include:

- powders, liquids emanating from package
- wrapping stained by liquid leakage
- unexpected items or materials found in package on opening or X-raying (loose or in a container) such as powdered, crystalline or granular solids; liquids; sticky substances or residues
- unexpected odours observed on opening
- sudden onset of illness or irritation of skin, eyes and nose

© NaCTSO Crown copyright 2017

## 3. WHAT YOU CAN DO

The initial step will be recognition that an incident has occurred (e.g. through the indicators described above), though the precise nature of the incident (e.g. CBR) may not be immediately apparent. The enactment of the response procedure will follow, including communication with the emergency services who will provide the appropriate response. Detailed below are some points to consider when planning your response procedure. Ensuring that the appropriate staff are familiar with your response procedure is key to its successful implementation.

- Ensure that forethought is put into communication with both staff and the emergency services.
- Ensure that doors can be closed quickly, if required.
- Pre-plan your evacuation routes, ensuring they do not lead building occupants through affected areas. Consider how you will communicate the evacuation routes to occupants during an incident. The level of evacuation may vary depending on the nature of an incident and may not require the evacuation of your entire building or site.
- Consult with your Building Services Manager on the feasibility of emergency shutdown or isolation of heating, ventilation and air conditioning (HVAC) systems (including local extraction systems e.g. in kitchens) and ensure that any such plans are well rehearsed.

Note: due to the complexity of HVAC systems and the variability across buildings and sites, it is not possible to provide generic advice on the alteration or otherwise of HVAC systems in response to an incident- consultation with your organisation's building services manager and/or specialist HVAC engineers is essential.

You do not need to make any special arrangements for medical care beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties. However, the provision of materials to undertake improvised decontamination (absorbent materials and water) in a suitable location (i.e. where you would likely evacuate contaminated staff to) may be appropriate.

### 3.1 Actions upon discovery of any suspicious delivered item

You could discover a suspicious item in a mail room, or anywhere else in the building- ensure you have appropriate emergency response plans in place.

### 3.2 Avoid unnecessary handling and X-raying:

- if you are holding the item, put it down on a cleared flat surface
- keep it separate so it is easily identifiable
- do not move it, even to X-ray it
- if it is in an X-ray facility, leave it there

### 3.3 Move away immediately

- clear immediate area and each adjacent room, including rooms above and below
- if there is any suggestion of chemical, biological or radiological materials, move those directly affected to a safe location close to the incident, keep these individuals separate from those not involved
- prevent others approaching or accessing the cleared areas
- do not use mobile phones or two-way radios in the cleared area or within fifteen metres of the suspect package
- communicate regularly with staff, visitors and the public

### 3.4 Notify police

- if the item has been opened, or partially opened prior to being deemed suspicious, it is vital that this is communicated to the police
- ensure informants and witnesses remain available to brief the police, and that the accuracy of their observations is preserved: encourage witnesses immediately to record their observations in writing, and discourage them from discussing the incident or their observations with others prior to the arrival of the police

© NaCTSO Crown copyright 2017

**3.5 Additional CBR-specific actions**

- if a CBR incident is suspected then undertake improvised decontamination of contaminated individuals as quickly as possible, ideally within the first 15 minutes
- in the event of a CBR incident occurring it is advised that lifts should not be used in order to move around, or evacuate the building
- if the alteration of the HVAC system features within your response plan (see note above), this should be undertaken as quickly as possible

## 4. PLANNING YOUR MAIL HANDLING AND SCREENING PROCEDURES

Although not all suspicious items will be hazardous or malicious, you may not be able to determine this without support from the emergency services. Therefore communication with the emergency services is important in triggering the appropriate response, as highlighted above.

A risk assessment is fundamental to ensuring that any measures or procedures your organisation implements are proportional to the risk it faces. Your local police Counter Terrorism Security Advisor (CTSA) can assist with this process by providing information to support threat and impact assessments, as well as relevant mitigation measures. Take the following into account in your planning:

- Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the building.
- Consider your organisational response should there be any changes to your organisations risk assessment or mail streams.
- Ensure that all staff who handle mail are briefed and trained in how to recognise and respond to the threats your organisation faces. Include reception staff and encourage regular correspondents to put their return address on each item.
- Ensure all sources of incoming mail (e.g. Royal Mail, couriers, and hand delivery) are included within your overall screening process. Note that not all mail streams may require the same level of screening (e.g. if it is deemed lower risk, such as internal mail).
- At present there are no CBR detectors capable of identifying all hazards reliably. Furthermore, while X-ray mail scanners may detect devices for spreading CBR materials (e.g. explosive devices), they will not detect the materials themselves. For further advice on CBR detection, contact your local CTSA.
- Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries.
- Consider the physical protective measures (e.g. blast protection, dedicated HVAC systems, specialist filtration, washing and shower facilities) you require to protect your organisation and those undertaking mail screening. These should be proportionate to the level of screening that is undertaken, but consider the highest anticipated level of screening that may be required, as physical protective measures may be challenging to alter in response to any change in threat.
- Make certain mail handling areas can be promptly evacuated. Rehearse evacuation procedures and routes as well as communication mechanisms which would be used throughout the incident.
- Staff who are responsible for mail handling should be made aware of the importance of isolation of themselves (in a safe location) and the mail item of concern (i.e. leave it where it is, do not transport this to another part of the building for further inspection) in reducing contamination.

**If in doubt call 999 and ask for the police. Clear the area immediately. Do not attempt to open the letter or package. Avoid unnecessary handling. Keep it separate so it is easily identifiable.**

Contact 999 and ask for the police

© NaCTSO Crown copyright 2017

**GO TO SECTION CONTENTS**

Read more about Evacuation, invacuation, lockdown, protected spaces

Go to the CPNI website

Go to the PAS 97:2015 Mail screening and security specifications

Go to the CPNI Screening mail and courier deliveries webpage

Go to Glossary

© NaCTSO Crown copyright 2017

# Hostile vehicle mitigation (HVM)

## 1. INTRODUCTION TO VEHICLE BORNE THREATS

**The threats range from vandalism to sophisticated or aggressive attack by determined criminals or terrorists.**

- vehicles offer a convenient method to deliver a bomb, known as a vehicle borne improvised explosive device (VBIED)
- a vehicle can also be used as a weapon to ram and damage infrastructure or to injure and kill people

## 2. VBIEDs

The effects from a VBIED include the blast, fireball, primary, and secondary fragmentation and ground shock. Blast stand-off (the distance between the explosive and the asset) is the single most important factor in determining the extent of damage that can be caused. This is site specific, it is important to maximise the blast stand-off distance.

**There are five main attack types when using a Vehicle Borne Improvised Explosive Device (VBIED):**

| | |
|---|---|
| **Parked** | A VBIED may be parked close to an asset that is the terrorist's target. The blast effects are far greater when the VBIED is closer to the asset. |
| **Encroachment** | A hostile vehicle may be able to exploit gaps in perimeter protection, or tailgate a legitimate vehicle through a single layer Vehicle Access Control Point (VACP). Alternatively a hostile can tamper with an active vehicle security barrier to open it in advance of an attack. |
| **Penetrative** | A vehicle may be used to weaken and/or breach a building or physical perimeter. A penetrative attack could result in an IED detonating inside a weakened structure. |
| **Deception** | A hostile vehicle may be modified to replicate a legitimate vehicle (i.e. "Trojan horse" vehicle), be an ex-fleet vehicle or the occupant(s) of a vehicle may use pretence to gain site access. |
| **Duress** | A security officer could be forced to open a vehicle access control point (VACP) or a legitimate driver could be forced to take an IED within their vehicle in to a vulnerable location. |

## 3. VEHICLE AS A WEAPON (VAW)

A vehicle by itself can also be used with hostile intent to breach a perimeter, ram and damage infrastructure, or as a weapon to injure and kill people. This is referred to as a 'vehicle as a weapon' attack. The use of VAW has been used by terrorists to target crowded places. A broad range of vehicles can cause significant loss of life and serious injury.

## 4. MITIGATING A VEHICLE BORNE ATTACK

Threats from vehicles can be mitigated by installing physical measures (including blending into the landscape or streetscape) which may be passive (static) or active (security controlled). These measures can be installed either on a permanent or temporary basis. All such measures should meet appropriate standards in terms of their vehicle impact performance, design and installation. This will depend on the operational requirements applicable to the site.

© NaCTSO Crown copyright 2017

### 4.1 Hostile Vehicle Mitigation (HVM) and Vehicle Security Barriers (VSBs)

HVM uses a blend of traffic calming measures to potentially slow down hostile vehicles and vehicle security barriers to stop those hostile vehicles progressing further. There are a variety of HVM and VSB options to assist reduce or mitigate the threat from vehicles.

These include:

- total traffic exclusion from an area, using VSBs
- traffic exclusion using VSBs, but with screening of all vehicles entering the area (with suitable VACP, preferably two layers of active VSB to prevent vehicle tailgating)
- traffic inclusion/free flow within an area but with all critical/vulnerable assets within that area protected with VSBs
- temporary/supplementary barriers installed at times of heightened threat or when a secure event is present in the area

### 4.2 The range of Vehicle Security Barriers includes:

- bollards (active retractable and passive static)
- gates
- planters and strengthened street furniture such as seating

### 4.3 Landscaping options include:

Ditches, bunds and berms.

The best form of HVM is total traffic exclusion from an area, which should be enforced by appropriately rated and correctly installed VSBs. A deployment of VSBs that restricts traffic (vehicles, pedestrians or both) requires an Anti-Terrorism Traffic Regulation Order (ATTRO) which is recommended to the traffic authority by the Chief Officer of Police.

Installing a static VSB system at a suitable standoff distance from a site will negate deception and duress styles of attack. It can also mitigate tampering and tailgating, which are forms of an encroachment attack.

If frequent vehicle access is required into a site then active solutions should be considered. Manual barriers require subsequent resourcing in terms of staffing and automated barriers require both proactive maintenance and reactive callout procedures. These solutions are generally more expensive and less secure than a static security barrier system for the reasons outlined above.

If sites are occasionally accessed by vehicles, then it may be more cost effective to use plant-removable barrier systems (for example a socketed bollard) rather than installing fully automated active.

## 5. TEMPORARY OPTIONS

### 5.1 Temporary VSBs

Modular wall units portal and gate units that can be interlinked to provide a surface mounted (gravity/free standing) or pinned solutions. Some systems can have pedestrian fences mounted on them to give dual purpose protection. Sites or police forces can rent VSBs on a temporary basis. To access these assets you should consult with your local CTSA.

### 5.2 Vehicles as a barrier

Following an appropriate **risk assessment,** you may consider the use of a vehicle as a barrier as possible mitigation against a vehicle as a weapon (VAW) attack. This should only be utilised following **advice from a SECCO or CTSA.** Such a deployment may impact upon the safety of the event e.g. emergency access, crowd flow rates, evacuation routes and the safety and security of the vehicle drivers must also be considered.

## 6. CONTINGENCY BARRIER SCHEMES

Repeated renting of temporary barriers is expensive; sites should therefore consider a contingency barrier scheme. These are typically pre-installed gated VSBs in the relevant areas, which can be closed just prior to the event or pre-installed foundation sockets in to which passive or active VSBs are slotted. This avoids the loss of lane availability during the installation of temporary barriers on the days/nights prior to an event, which can bring benefits to the communities and transport authorities.

## 7. STANDARDS AND TESTING

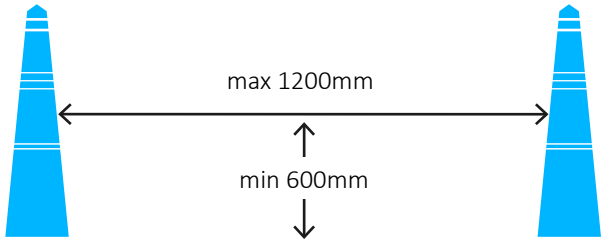
The impact test standards for VSBs are IWA14–1 and PAS68, both of which include a range of test vehicles

© NaCTSO Crown copyright 2017

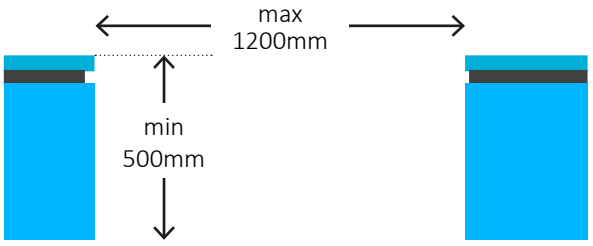
ranging from 1.5t cars, through 2.5t 4x4s, 3.5t vans, 7.2/7.5t trucks to 30t trucks. The results of the tests are classified in terms of how far the vehicle penetrated beyond the VSBs. This “penetration distance” is crucial, particularly when sites have limited standoff between the VSB and asset. Temporary barriers tend to displace more than permanently installed VSBs, as they do not have the benefit of a structural foundation.

Not all sites require protection from the largest or fastest vehicle-borne threats as the local topography or threat assessment may preclude them. Police CTSAs or skilled security consultants including the Register of Security Engineers and Specialists (RSES) with access to CPNI materials can assess the maximum impact speeds, by carrying out a vehicle dynamics assessment; these should be used to scope the most suitable VSBs, and/or quantify the residual risks.

## TECHNICAL REQUIREMENTS




The maximum clear distance between adjacent VSB must be no greater than 1200mm, this distance must be measured between structural elements at a height of 600mm above ground level.




The minimum height for vertical fixed structure is 500 mm. An increased height of 900 mm will make the measures more conspicuous

GO TO SECTION CONTENTS
Go to the CPNI Hostile Vehicle Mitigation webpage
Go to Glossary

© NaCTSO Crown copyright 2017

# Digital built assets and environments

## 1. INTRODUCTION

Digital built assets and environments generate digital representations of, and data and information about, physical and functional aspects of a built asset which can be used throughout its lifecycle. It requires a much more cross-sector collaborative approach that has traditionally been seen in the architectural, engineering and construction industries, with more transparent, open ways of working and sharing of detailed models and large amounts of digital asset information.

A built asset may comprise of a building, multiple buildings (e.g. on a site or campus), a portfolio or network of assets, or built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) and may include associated land or water.

Asset information refers to data or information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization. Asset information can include design information and models, documents, images, software, spatial information and task or activity-related information.

The planning, design, construction, operation and maintenance of built assets is increasingly making use of digital engineering and placing greater reliance on digital technologies. It is important that security managers understand the inherent vulnerability issues which arise. This may be through unauthorised, or malicious use of authorised, access to systems critical to the safety, security and resilience of: personnel and other occupants or users of the built asset and its services; the built asset itself; asset information; and/or the benefits the built asset exists to deliver, be they societal, environmental and/or commercial.

> Policies and processes need to be in place to encourage the adoption of appropriate and proportionate controls if the trustworthiness and security of digital built assets is to be maintained.

## 2. SECURITY OF DIGITAL BUILT ASSETS

The models and the associated databases will contain large amounts of aggregated information about a built asset including:

- its design and associated specifications
- the construction process
- component assets, their precise location and interconnectivity
- product data about component assets including specification, design and maintenance information
- the services or function the built asset provides
- its occupants or users
- operational and management procedures, including those relating to safety and security

Alongside the developments in digital engineering there is a drive to make public data more easily accessible unless there are clear and specific reasons not to do so. This is likely to increase the amount of information available in the public domain.

The use of Building Management Systems (BMS) is already commonplace. However, with technology used by most BMS and third party systems starting to converge, the increasing use of Internet Protocol (IP) networks by systems to communicate internally and with the outside world, and the use of commercial off-the-shelf IT products, software and operating systems as key components, a number of potential vulnerabilities are created.

© NaCTSO Crown copyright 2017

### 3. PAS 1192 – 5:2015

Access to any of the types of information and systems described above would greatly assist those engaged in a range of criminality activity, espionage and terrorism. In order to understand and address those potential vulnerabilities the Centre for the Protection of National Infrastructure (CPNI) and the British Standards Institution (BSI) have produced guidance, PAS 1192 – 5:2015, Specification for security-minded building information modelling, digital built environments and smart asset management.

The standard sets out effective and proportionate ways to enable the safe and secure sharing and publication of digital asset information. It is supported by a suite of related guidance documentation available on the CPNI website.

Go to the BSI PAS: 1192-5:2015 webpage

**GO TO SECTION CONTENTS**

Go to the CPNI Digital built assets and environments webpage

Go to Glossary

© NaCTSO Crown copyright 2017

# Personnel and people security introduction

## 1. PERSONNEL AND PEOPLE SECURITY

### 1.1 What is personnel security?

Personnel security is a system of policies and procedures which seek to manage the risk of people exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes. These purposes can encompass many forms of criminal activity, from minor theft through to terrorism.

The purpose of personnel security is to minimise the risks. The recommended action for doing this is firstly to identify the people risks within your organisation by conducting a personnel risk assessment. Follow this by implementing thorough pre-employment screening methods to employ only suitably qualified and reliable individuals. Once emplyed, manage them well to minimise the chances of staff becoming disgruntled. Finally, create a strong security culture, detect suspicious behaviour, and resolve security concerns once they become apparent.

### 1.2 The Insider Threat

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

An insider could be an employee, contractor, agency staff or even a business partner who has authorised access to your assets. They may already be working for you and see an opportunity to conduct an insider act for their own benefit, or may be someone newly joined who has infiltrated your organisation in order to seek information. They may be someone who has been coerced by a third party to exploit the access their job might provide.

Go to the CPNI Reducing insider risk website

### 1.3 Risk assessment process

Your organisation needs to have a risk management process in place which manages the consequences of an unauthorised or unlawful act and a process in place that helps you:

- identify and analyse the root cause of the incident
- identify the appropriate disciplinary actions or interventions that need to be undertaken
- assess the effectiveness of current control measures in place
- identify gaps in practice
- develop more effective control measures

These processes help your organisation learn from the incident and put in place measures to prevent the incident from occurring again.

Go to the CPNI Insider risk assessment website

## 2. PRE-EMPLOYMENT SCREENING

Personnel security involves a number of screening methods, which are performed as part of the recruitment process but also on a regular basis for existing staff. The ways in which screening is performed varies greatly between organisations; some methods are very simple, others are more sophisticated. In every case, the aim of the screening is to collect information about potential or existing staff and then to use that information to identify any individuals who present security concerns in a proportionate way.

Pre-employment screening seeks to verify the credentials of job applicants and to check that the applicants meet preconditions of employment (e.g. that the individual is legally permitted to take up an offer of employment). In the course of performing these checks it will be established whether the applicant has concealed important information or otherwise misrepresented themselves. To this extent, pre-employment screening may be considered a test of character.

### 2.1 Pre-employment checks

Personnel security starts with the job application, where applicants should be made aware that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and could amount to a criminal offence. Applicants should also be made aware that any offers of employment are subject to the satisfactory completion of pre-employment checks.

If an organisation believes there is a fraudulent application

© NaCTSO Crown copyright 2017

involving illegal activity, the police should be informed. Pre-employment checks may be performed directly by an organisations Human Resources Department, or this process may be sub-contracted to a third party. In either case the organisation needs to have a clear understanding of the thresholds for denying someone employment. For instance, under what circumstances would an application be rejected on the basis of their criminal record, and why? Organisations using a third party for screening purposes should conduct regular audit checks to ensure the screening is meeting the standards required.

**2.2 Data Protection Act**

The Data Protection Act (DPA) (1998) applies to the processing of personal information about individuals. Personnel security measures must be carried out in accordance with the data protection principles set out in the act.

**2.3 Pre-employment screening policy**

Your pre-employment screening processes will be more effective if they are an integral part of your policies, practices and procedures for the recruiting, hiring, and, where necessary, training of employees. If you have conducted a personnel security risk assessment then this will help you to decide on the levels of screening that are appropriate for different posts.

**2.3.1 Identity**

Of all the pre-employment checks, identity verification is the most fundamental. Two approaches can be used:

- A paper-based approach involving the verification of key identification documents and the matching of these documents to the individual.
- An electronic approach involving searches on databases (e.g. databases of credit agreements or the electoral role) to establish the electronic footprint of the individual. The individual is then asked to answer questions about the footprint which only the actual owner of the identity could answer correctly.

Pre-employment checks can be used to confirm an applicant's identity, nationality and immigration status, and to verify their declared skills and employment history.

The Immigration, Asylum and Nationality Act 2006 means there are requirements of employers to prevent illegal working in the UK. These include an ongoing responsibility to carry out checks on employees with time-limited immigration status. Failure to comply with these regulations could result in a possible civil penalty or criminal conviction.

Go to the CPNI Pre-employment screening webpage

**2.3.2 Qualifications and employment history**

The verification of qualifications and employment can help identify those applicants attempting to hide negative information such as a criminal record, poor performance or dismissal. Unexplained gaps should be explored during the recruitment process.

**2.3.3 Qualifications**

When confirming details about an individual's qualifications it is always important to:

- consider whether the post requires a qualifications check
- always request original certificates and take copies
- compare details on certificates etc. with those provided by the applicant
- independently confirm the existence of the establishment and contact them to confirm the details provided by the individual

**2.3.4 Employment history**

For legal reasons it is increasingly difficult to obtain character references, but past employers should be asked to confirm dates of employment and role undertaken. Where employment checks are carried out it is important to:

- check a minimum of three but ideally five years previous employment
- independently confirm the employer's existence and contact details (including the line manager)

© NaCTSO Crown copyright 2017

- confirm details (dates, position, salary) with HR
- where possible, request an employer's reference from the line manager

**2.3.5 Criminal record checks**

A criminal conviction – spent or unspent – is not necessarily a bar to employment. However, there are certain posts where some forms of criminal history will be unacceptable. To obtain criminal record information, a company can request that an applicant either:

- completes a criminal record self-declaration form
- applies for a Basic Disclosure certificate

Go to the Government Disclosure and barring service webpage

**2.3.6 Role specific checks**

For some posts it may be justifiable to carry out medical, financial or social media checks. For example where the employee's position requires the handling of money, financial checks would be appropriate. Interpreting the security implications of role specific checks is not straightforward and will require each organisation to decide where their thresholds lie (e.g. in terms of an acceptable level of debt) and specialist expertise in the area being checked.

**2.3.7 Overseas checks**

As the level of outsourcing rises and increasing numbers of foreign nationals are employed in the UK, it is increasingly necessary to screen applicants who have lived and worked overseas. As far as possible, organisations should seek to collect the same information on overseas candidates as they would for longstanding UK residents (e.g. proof of residence, employment references, criminal record). It is important to bear in mind that other countries will have different legal and regulatory requirements covering the collection of information needed to manage personnel security and therefore this step may be difficult. A number of options are available to organisations wishing to perform overseas checks:

- request documentation from the candidate
- hire professional/ an external screening service
- conduct your own overseas checks

In some circumstances you may be unable to complete overseas checks satisfactorily (e.g. due to a lack of information from another country). In this case, you may decide to deny employment, or to implement other risk management controls (e.g. additional supervision) to compensate for the lack of assurance.

Go to the CPNI Overseas criminal record checks guidance

## 3. ONGOING PERSONNEL SECURITY

While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually or in response to events. CPNI's Insider data collection study identified:

- Over 75% of the insider acts were carried out by staff who had no malicious intent when joining the organisation, but whose loyalties changed after recruitment.
- In many circumstances the employee undertaking the insider act had been in their organisation for some years prior to undertaking the activity and exploited their access opportunistically.
- CPNI's collection of ongoing personnel security guidance and tools can be used to help an organisation develop and plan effective practices for countering the insider threat and maintaining a motivated, engaged and productive workforce.
- The application of good ongoing personnel security principles adds huge value to physical and technical security measures in a cost effective manner, promoting good leadership and management and maximising people as part of the security solution.

Go to the CPNI Ongoing personnel security good practice guidance

© NaCTSO Crown copyright 2017

## 4. INVESTIGATION AND DISCIPLINE

Many organisations will at some point need to carry out some kind of internal investigation into a member of staff. The primary duty for an investigator is to establish the true facts, whilst adhering to appropriate HR policy and employment laws.

Organisations can react disproportionately to accusations, which can lead to costly employment tribunals or an unhappy and disaffected workforce. Conversely, organisations which fail to take any appropriate investigative and subsequent disciplinary action can create a culture where staff actively disregard security policies and processes.

With correct procedures in place employees who understand policies and regulations, and competent trained investigative staff, your organisation is better equipped to avoid these pitfalls and maintain trust.

Go to the CPNI Investigating employees of concern guidance

Go to the CPNI Personnel security risk assessment guide

## 5. SECURE CONTRACTING

Contractors present particular personnel security challenges. For instance, the timescales for employing contractors are often relatively short, and there is greater potential for security arrangements to be confused or overlooked (e.g. due to further sub-contracting).

In managing the insider risks associated with contractors it is important to:

- Ensure that pre-employment checks are carried out to the same standard as for permanent employees. Where this is not possible, due to tight deadlines or a lack of information available for background checking, then the resulting risks must be managed effectively. Preferably the implementation of any additional security measures will be guided by a personnel security risk assessment.
- Where pre-employment checks- or any other personnel security measures are carried out by the contracting agency rather than the employing organisation, a detailed account of the checks to be undertaken and the standards achieved must be incorporated into the contract that is drawn up between the two. Furthermore, the pre-employment checking process conducted by the contractor should be audited regularly.
- Confirm that the individual sent by the contracting agency is the person who arrives for work (e.g. using document verification or an electronic identity checking service).

Once the contractor has started working for the organisation, they will need to be managed securely. The following steps will help:

- Carry out a risk assessment to establish the threats and level of risk associated with the contractor acting maliciously in post.
- Ensure that the contract exists, either between the organisation and the contractor, or between the organisation and the contracting agency, defines the codes of practice and standards that apply.
- Provide photo passes to contract and agency staff, and stipulate that they must be worn at all times. Ideally, the employing organisation should retain contractors' passes between visits, reissuing them each time only after the contractor's identity has been verified.
- The employing organisation and the contracting agency (or the contractor, if no agency is involved) should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contract between the two parties, and the employing organisation will need to decide what additional personnel security measures to implement- for example, restricted or supervised access - when the replacement is on site.
- Where a contractor is in post but the necessary pre-employment checks have not been carried out- or where the results of the checks are not entirely positive but the need for the contractor's expertise is such that

© NaCTSO Crown copyright 2017

they are employed anyway- then additional personnel security measures must be considered (e.g. continuous supervision).

## 6. REMOTE WORKING

Remote Working brings advantages for both the employer and employee including retention of motivated staff, increased flexibility and autonomy, and reduced costs for the organisation through consolidating and reducing office space. However, it also brings a number of people security issues which, if left unchecked, could lead to employee disaffection and increase the risk of counter productive work behaviours and malicious activity. These might include:

- increased security risks resulting from the loss of IT equipment or sensitive company data, living in shared accommodation
- direct supervision of employees is not possible, with potential security or welfare concerns going unchecked
- perception by the remote worker of loneliness and isolation, and being left 'out of the loop'
- performance issues including the possibility of both under and over working, and resulting management issues

Go to the CPNI Ongoing personnel security webpage

## 7. SECURITY CULTURE

Effective security relies on people behaving in the right way. This is enabled through an understanding of the threat and a clear understanding of what is required of them. In this way, an organisation's people play a significant role in the detection, deterrence and prevention of security threats.

The development of an appropriate security culture, where the right security behaviours are adopted by the workforce, is essential to an organisation's protective security regime. Used the right way, your staff, guard force, contractors, visitors, suppliers and the general public can be a huge force multiplier, at a relatively low cost, in strengthening your resilience to security threats and reducing your vulnerability to attack

Security culture is defined by CPNI as 'the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security'.

Without the right security values (i.e. culture), employees may pay lip service to the security practices in place, resulting in poor behaviours and lack of compliance with protective security measures. This in turn can lead to increased risk of security incidents and breaches, reputational and financial damage, the development of a climate that facilitates insider threat, as well as potential harm to employees, customers, and/or business performance.

Before embarking on a change programme, however big or small, it is critical that an organisation is clear on the following:

- the objectives of the change (i.e. the vision or strategy)
- the size and scale of the change (i.e. the gap between where the organisation is now and where it wants to be)
- the actions to implement the change (i.e. the interventions)
- the organisation is ready for the change (i.e. it has the necessary time, resources and buy-in)
- how to communicate the change to the target audience and other key stakeholders (i.e. the communications strategy)
- how to review and evaluate the impact of the change (i.e. the measures of success and key performance indicators)

Embedding and maintaining change takes times. It also requires a clear vision, as well as a coordinated strategy to ensure the interventions are consistent, practical and meaningful.

© NaCTSO Crown copyright 2017

There is no one right way to deliver change. The approach to take will depend on whether you are embedding behaviour change or culture change, the current climate in your organisation, and what will resonate most with your target audience. A bespoke approach, suited to the particular needs and requirements of your organisation will ultimately work best.

**GO TO SECTION CONTENTS**

Go to the CPNI Embedding security behaviour change webpage

Go to the CPNI Ongoing personnel security infographic

Go to Glossary

© NaCTSO Crown copyright 2017

# Personnel security training and good practice

## 1. INTRODUCTION PERSONNEL SECURITY TRAINING

Following a risk assessment you can evaluate if it is necessary to employ a guard force as part of your security plan. It is important that security staff understand their roles and responsibilities and are properly tasked, trained and participate in rehearsal exercises. It is desirable that individuals working in the security industry undergo a structured training program that results in a recognised qualification, in some sectors training is a mandatory requirement.

Supervision of staff is fundamental in order to be effective and deliver your intended outcomes. Capability, capacity, competence and reliability of staff are particularly important in relation to counter-terrorism. Within this guidance we have identified some of the skills staff require to remain alert, communicate effectively, patrol effectively, respond to suspicious items, bomb threats, hostile reconnaissance and firearms and weapons attacks for example. A strong security culture within your organisation, beginning at senior management level, will assist your staff to not only disrupt terrorist attack planning but also prepare them should an incident occur.

It is vital that security staff patrol regimes for sites and events are also outwardly facing, look beyond the perimeter before the event, during and post event. The security patrol regime will complement the deterrence communication messaging and search planning. Supervisors are key to ensure levels of vigilance are maintained throughout the life cycle of any event.

Go to the CPNI Professionalising security webpage

**Key principles of developing and maintaining an effective workforce**

The majority of personnel will not retain all the information provided to them, with many retaining as little as a 5% of the information within the immediate 24hour period. Therefore it is important that training and briefings are regular, clear and appropriate to reinforce key messages and instructions. Skills and knowledge in relation to security can then be developed and maintained (this need is supported by academic research on information retention). For this purpose a blended style of training is shown to be more effective. Begin with a training needs analysis followed by individual training, collective training and rehearsal exercises. Collective training will make the whole greater than the sum of the parts. Competent people and effective teams are the bedrock of a reliable incident response and adapting flexibly to the unexpected.

As an organisation you should have identified the people or department responsible for the development of your security plan. All staff not just those responsible for security should have a clear understanding how the elements of security will better protect your business.

## 2. TRAINING A WORKFORCE TO MAINTAIN PROTECTIVE SECURITY.

You should consider the following elements to deliver an effectively trained workforce in relation to security:

- training should be based upon the current policy and standards
- assess your training requirements
- appropriately tailored security training is provided to all staff as part of the organisation wide security responsibility and culture
- ensure you provide leadership, management, mentoring and communication training for supervisors to facilitate on going staff development
- staff turnover should be taken into account in detailed training plans, to ensure that new staff are trained and existing staff receive appropriate refresher training
- prepare a training plan for the following 12 months, building in a time line for refresher training
- training activity should be flexibly delivered in various formats such as formal classroom, online off shift on staffs personal IT, online during shift with support, face to face debriefs post incident or through the organisations intranet
- ensure staff are trained before you put them through rehearsal and validation exercises

© NaCTSO Crown copyright 2017

- include counter terrorism awareness training on the induction programme, for larger organisations, this may involve the local Counter Terrorism Security Advisor or Counter Terrorism Awareness Advisor
- provide briefings to all personnel on organisational security updates
- training should be provided on a continuous basis to prepare staff
- ensure security awareness is included on your staff induction day. Set your intention out from the commencement of employment and create a strong security culture and positive reporting culture in the organisation

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

- initial actions at a terrorist incident
- the different terrorist threat levels, building response levels and different activities required should there be an increase in threat
- hostile reconnaissance, how to patrol effectively to disrupt activity, identify and respond to suspicious behaviour
- suspect items, the 'four Cs' protocols and the HOT principles
- chemical, biological and radiological incidents, how to recognise and respond using STEPS 123
- a firearms and weapons attacks and the Run, Hide, Tell principles
- evacuation, invacuation and lockdown procedure demonstrating knowledge of the emergency assembly points
- how to search a site effectively
- the basic principles of good housekeeping and how it reduces the opportunities for an attack
- how to respond appropriately to a bomb threat
- how and when to report incidents either to the internal security team, calling police using 999, 101 or call the Anti-Terrorist Hotline 0800 789 321. Staff should understand the reason why they use either 999 or Anti-Terrorist Hotline
- using emergency equipment such as defibrillators etc. as trained
- use of incident logs and checklists that facilitate an effective response to incidents such as terrorist incidents, bomb threats etc.

> Ensure you maintain your search and patrol regime for the lifecycle of the event including prior to the commencement, during and post event. Consider a patrol sweep of the public areas before, during, ten minutes prior to the conclusion of an event and post-event. Look for suspicious items and behaviour. Patrol areas might include areas close to the site, pick up zones and transport hubs. Ensure those patrol staff can communicate effectively with a control room.

(Integrating the CPNI staff vigilance campaign supplies organisations with materials to facilitate internal policies and procedures)

You may want to complete the ETHANE checklist

Read more about Suspicious items

Read more about CBR attacks

## 3. SUPERVISORS TRAINING AND ROLE IN QUALITY ASSURANCE AND DEVELOPMENT OF THE WORKFORCE

Security supervisors are key enablers to ensure you have a motivated effective guard force that perform to the required standards and achieve the security aims and objectives of the organisation. Effective leadership by individuals during recent terrorist attacks has saved lives. The following factors should be considered when training your security supervisors.

© NaCTSO Crown copyright 2017

**3.1 Supervisors training**

- Allocate time to allow supervisors to actively supervise and engage with their staff.

By providing sufficient time to supervisors they will develop a knowledge of their team and their individual and collective capability.

- Provide supervisors with the right information and materials to continually develop and reinforce learned behaviours, knowledge and skills of their allocated staff.

On-going reinforcement of competencies is required for all staff to achieve and maintain standards.

- The organisation should provide leadership, management, mentoring and communication training for supervisors.

Leadership and management training will facilitate the development of a diverse workforce and may improve retention rates and absentee levels.

- Have a training programme for supervisors to regularly attend counter terrorism awareness training such as Project Griffin and Project Argus.

By providing the on-going up skilling and current counter terrorism information to supervisors, they will be able to support the skills and knowledge of their staff.

- Ensure supervisors have access to useful information from the NaCTSO, CPNI and MI5 websites.

Supervisors can share the latest information and guidance with their staff as part of briefing activity to keep them up to date.

- Security supervisor should quality assurance and develop the guard force.

Supervisors are well placed to understand the skill set of their staff and identify opportunities for development

**3.2 Supervisors role to quality assure and develop the workforce**

- Ensure staff outline their roles and responsibilities from a counter terrorism safety and security perspective.

Clear definition of roles will support the right person to take the lead role when dealing with incidents and facilitate the delivery of the incident management plan. Where staff have attended rehearsal exercises their understanding of their role and responsibility and confidence to respond increases.

- Ensure staff regularly use training materials, including online to improve their knowledge and understanding.

By using these materials during the induction process, staff will have a better understanding of the organisations security plan and receive practical guidance how to respond effectively to security issues

- Supervisors should have a full understanding and record of the qualifications their staff have obtained and should revisit the competencies.

By revisiting these competencies achieve in the qualifications staff knowledge is reinforced and retained

- Ensure your staff regularly receive of counter terrorism awareness training such as Project Griffin.

We know personnel require a regular reminder of principles in order that they will become confident and competent in the identification, challenge and reporting of suspicious behaviour

- Following appropriate training ensure rehearsal exercises prepare staff for the identification and response to incident such as suspicious behaviour, suspicious items (IEDs, mail, chemical biological radioactive material) etc.

Integrating the CPNI staff vigilance campaign supplies organisations with materials to facilitate staff training

- Ensure training and rehearsal exercises are regular.

Regularly training and rehearsal exercises you will prepare staff in identifying and responding to critical incidents such as a terrorist attack, communicate and respond more effectively. Staff gain confidence to become effective during an attack and remain vigilant for a longer periods of time

- Provide first aid training to your staff.

© NaCTSO Crown copyright 2017

By providing first aid training, staff will be responsive to the use of emergency equipment e.g. defibrillators, and will be first responders to any injured personnel.

- Train and rehearse you staff in your emergency plan with personnel which supports an evacuation, invacuation and lockdown procedure.

By creating and sharing the emergency plan staff should identify all assembly points and procedures in the event of an evacuation, understand where the protected spaces are located during an invacuation, be familiar with their site to marshal and support an evacuation, invacuation and understand how to lockdown a facility or event

- Are staff trusted to use their judgement based upon the information they have?

It is essential that staff understand their roles and responsibilities. Supervisors who are part of the design of the security plan will be best placed to respond during the threat. Regular training and rehearsal exercising activity will support the decision making process for all staff.

- Ensure the organisations' security plan, policies and changes in procedures are shared by supervisors.

Supervisors can mentor and coach staff to reinforce positive behaviours within the context of the organisation security plan.

You may want to complete the ETHANE checklist

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Hostile reconnaissance

## 1. INTRODUCTION

### 1.1 Overview and aim of this guidance

Hostile reconnaissance is the term given to the information gathering phase by those individuals or groups with malicious intent, it is a vital component of the terrorist attack planning process. This guidance will explain why and how hostile reconnaissance is conducted and the principles of how to disrupt threats during the reconnaissance phase, along with practical measures on how to reduce the vulnerability of a site.

Information about a site or event is gained by using online research, on-site visits and if and where necessary, insider knowledge. The hostile will try to obtain enough detailed information and get sufficient certainty about the reliability of this information to inform their method of attack to be sure of success.

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

CPNI defines hostile reconnaissance as “Purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target.” Generally, the more sophisticated the attack the more complex the attack planning, and consequently the greater the information requirement and reconnaissance need.

### 1.2 Objectives of Hostile Reconnaissance:

- identify a TARGET
- discover WEAK SPOTS (vulnerabilities)
- assess the level and type of SECURITY
- determine the best METHOD OF ATTACK
- determine the likelihood of SUCCESS
- determine the best TIME to conduct the attack

## 2. HOW DO YOU IDENTIFY SUSPICIOUS BEHAVIOUR?

You must understand what is normal, what is every day. Take time to understand your working environment, the regular commute, the daily routine and the people and activities you see most often. Learn to spot the difference between normal and unusual/suspicious behaviour. Be alert to the threat.

### 2.1 What kinds of behaviour could be seen as suspicious?

- Is that person really taking a selfie or a photograph of something else?
- Are they loitering in restricted or non-public areas?
- Paying significant interest to entrances, exits, CCTV cameras or security features or staff?
- Asking unusual questions?
- Concealing their faces or in disguise?

It is not just people on foot, vehicles are often used by terrorists planning attacks. Be aware of vehicles parked out of place or left abandoned, or a vehicle retracing the same route.

### 2.2 Challenging and reporting suspicious behaviour

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

**Always remember - Stopping a terrorist before they can carry out their plans will save lives.**

You cannot spot a terrorist from their appearance, age, ethnicity, gender or clothing.

You can identify and report their suspicious behaviour.

### 2.3 What information do the police need from you?

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

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

© NaCTSO Crown copyright 2017

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

> **Remember:** it is always better that police are called while the person or vehicle is still at the scene

**2.4 Photography – Security staff powers**
**If part of the suspicious behaviour involves the taking of photographs, undertand your powers:**

- there is **NO** power in law to prevent a person from taking a photograph of anything or any person in a public place
- there is **NO** legal power to require or ask that any images taken are to be deleted
- security personnel have **NO** legal power to ask to view images taken
- security personnel have NO legal power to seize any camera or phone used to take any image
- if police are called, a person **CANNOT** be detained by security staff awaiting the arrival of police
- powers to search and seize are **ONLY** available to a **Police Officer**. (S.43 of the Terrorism Act 2000)

## 3. SECURITY MANAGERS

What are your trying to achieve?

- **Deny** the hostile the opportunity to gain information.
- **Detect** them when they are conducting their reconnaissance.
- **Deter** them by conveying failure through messaging and physical demonstration of the effective security.

This approach will play on their concerns of failure and detection.

The key to disruption comes from understanding the information hostiles need, and where they are going to have to go to get this and their state of mind. This, in turn, is dependent on understanding the threats in a way that enables prediction of likely attack scenarios.

> **Remember:** Deter + Deny + Detect = Disrupt

**3.1 DETER countering hostile reconnaissance: the principles**

Deterrence is a vital component of disrupting hostile reconnaissance. Deterrence is, for a majority of sites and organisations, the main desired effect of their protective security on hostiles.

Understanding the threat can allow a security manager to determine:

- what information the hostiles will be looking for and why?
- where the hostiles will go to obtain this information?

**3.2 DENY them what they need**

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

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

© NaCTSO Crown copyright 2017

### 3.3 DETECT and the state of mind of the hostile

Vigilant and engaged security officers with timely and appropriate response, can be particularly powerful.

As such, hostiles have a natural underlying anxiety about being detected which can alter their perceptions. For example, a CCTV camera directed on their position or a customer service representative coming up to them and innocently asking 'Are you OK there? Can I help you?" can be readily but incorrectly interpreted by them that they have been detected. This can disrupt hostile reconnaissance.

## 4. THE INSIDER THREAT

If the hostile is unable to gather the information, they require from online or on-site reconnaissance, they may attempt to recruit an insider to help achieve their aims.

To help mitigate the threat of insiders, a range of personnel security guidance is available from CPNI or your CTSA based on the following four components:

- personnel security risk assessment
- pre-employment screening
- ongoing personnel security (aftercare)
- security culture

When applied consistently, personnel security measures not only reduce operational vulnerabilities, they can also help build a hugely beneficial security culture at every level of an organisation.

### 4.1 Robust personnel security helps organisations to:

- Employ reliable people to minimise the chances of staff becoming unreliable once they have been employed.
- Detect suspicious behaviour and resolve security concerns once they emerge.

### 4.2 Examples of 'insider activity'

- unauthorised disclosure of sensitive information to a non-entitled third party
- process corruption (illegitimately altering an internal process or system to achieve a specific, non-authorised objective)
- facilitation of third party access to an organisation's assets (including premises, information and people)
- physical sabotage
- electronic or IT sabotage

### 4.3 What is an 'insider'?

| | |
|---|---|
| **Deliberate insider** | Obtain employment with the deliberate intent of abusing their access. |
| **Volunteer/ self-initiated insider** | Obtain employment without deliberate intent to abuse their access, but at some point personally decide to do so. |
| **Exploited/ recruited inside** | Obtain employment without deliberate intent to abuse their access, but at some point are exploited or recruited by a third party to do so. |

ACT ACTION COUNTERS TERRORISM

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Document awareness

## 1. THE THREAT

Terrorist and criminal organisations have the capability to print false passports and other identity documents. These can be used to enter the UK illegally, obtain employment, banking, housing, access to sites and hire vehicles for unlawful purposes as a few examples. Terrorists have used false identities when planning attacks.

## 2. IDENTITY DOCUMENT FRAUD

Identity document fraud can be conducted in a number of ways. Most cases of identity document misuse relate to passport fraud.

- imposters – where the holder of the document may look like the rightful owner
- counterfeit – a document made from scratch
- forgery – a genuine document which has been altered

### 2.1 Imposters

This is the simplest type of document fraud, where the 'holder' is simply a look-a-like, and the document is often not altered at all.

### 2.2 Counterfeits

A counterfeit document is one that has been made from scratch to resemble an officially issued document. The quality of counterfeits can vary greatly. High quality counterfeits can be difficult to identify.

### 2.3 Forged documents

A forged document is a genuine document which has been altered for a criminal purpose. Altering photographs and personal details are common examples but pages, visas and stamps may also be forged.

## 3. DOCUMENT VERIFICATION

Document verification is the process of ensuring that documents presented are genuine and that the holder is the rightful owner. It is also an integral part of the pre-employment screening process. Staff responsible for checking documents should be provided with the knowledge and tools needed to confirm the authenticity of documents, and identify basic forgeries. It is important that your document verification processes are integrated within your wider Pre-Employment Screening policies.

## 4. TRAINING

You should consider the training needs of staff who check documents, specifically:

- How much knowledge/experience do they already have?
- What sort of training might they require?
- How frequently should this training be refreshed?

## 5. DOCUMENT CHECKING

It is essential that all documents are examined thoroughly. The document verification process should be explained to all applicants as part of the recruitment process, highlighting which documents are requested and why, e.g. to guard against identity fraud and forgery. It is important to outline how important document verification is to your organisation and that you will seek to confirm the authenticity of relevant documentation.

Application processes must make it clear that applicants who cannot provide the required documentation will not be employed (except for cases where a reasonable explanation can be provided), particularly where their right to work in the UK must be verified.

## 6. EQUIPMENT

You should consider whether your processes require the use of verification tools. Both magnifiers and ultraviolet (UV) light sources are inexpensive and easy to obtain and will enhance your ability to detect fraudulent documentation. However, the use of this equipment will only be effective if users have a sound understanding of the document and its safeguards.

© NaCTSO Crown copyright 2017

**GO TO SECTION CONTENTS**

Contact the police or your local immigration office if you encounter a suspected false document

Contact NaCTSO for further information about the NaCTSO Document Awareness Workshop

Contact NaCTSO to get a copy of the Take Another Look DVD

Go to the National Document Fraud Unit: A good practice guide

Go to the PRADO – European Document Information website

Go to the Enforcement Office website

Go to Glossary

© NaCTSO Crown copyright 2017

# Guidance for commercial vehicles and hire companies

## 1. INTRODUCTION

Significant numbers of public service vehicles (PSV) and heavy goods vehicles (HGV) or their loads are stolen every year. A third are stolen for their loads and a third are stolen from the owner's premises. The primary reason is crime, however there is a crossover with terrorism where vehicles can be used as a weapon or funds from criminal activity can be used to finance terrorism. Most instances of crime are opportunist, however even simple precautions can make a difference. Where there is no security manager, it is important that a senior manager in a company has responsibility for security.

Companies hiring vehicles must also be responsible for ensuring they maintain the highest standards for verifying the identities of any business or drivers using their vehicles. Always examine the driving licence and ensure the photograph matches the driver, the licence is valid and in date. Two forms of identification are preferable. Take a copy or details of the licence (i.e. driver number) where possible.

Report all suspicious behaviour to the police.

The following advice is recommended to help detect, deter or deny those considering using a vehicle for criminal or terrorist purposes.

Call 999 to report suspicious behaviour to the police

## 2. ASSESS YOUR RISK

It's important that you, your colleagues and your employees understand the threat and recognise situations where you are vulnerable both in the UK and travelling abroad. Drivers are potentially vulnerable when parked off the road. There are many creative ways and means to target drivers and their vehicles. The objective may be to steal the vehicle or its load; cause specific loss to a business or its reputation; or to use the vehicle as a weapon.

## 3. RECRUITMENT

- always check a driver's references and previous five to ten year employment history
- always speak to previous employers (do not rely on phone numbers given by the driver)
- inform applicants that false details on application forms may lead to dismissal
- check driving licenses are valid and look for endorsements before you employ someone, and then at six-monthly intervals afterwards. Drivers should tell you of any changes to their license
- check if the applicant has any prosecutions pending or is waiting for sentencing by a court
- for agency drivers, ensure that the agency has carried out all of these checks including criminal records checks
- use only reputable agencies that are affiliated with a recognised UK trade organisation

Read more about Document awareness

## 4. COMPANY POLICY AND PROCEDURES

Build security duties and responsibilities into your company's contract of employment. Contracts should make clear that drivers will face disciplinary proceedings if they fail to carry out these duties.

Your company should:

- include your company's security instructions in the driver's induction and driver's handbook
- use photo identification cards for your company's drivers
- keep copies of all drivers document for your personnel records
- conduct due diligence checks on the identity of anyone hiring a vehicles, for HGVs and PSVs always insist on an operator's license where appropriate
- adopt a low tolerance approach to overdue rentals and hiring, report these to police at the earliest opportunity

© NaCTSO Crown copyright 2017

- ensure drivers communicate delays in arrivals to their destinations within agreed timeframes
- when drivers and staff leave ensure that they no longer have access to IT, keys, and information, change lock passcodes at regular intervals
- have a social media policy that outlines what staff, drivers and passengers can place on social media platforms
- consider using the Road Haulage Association's Security Audit Service

Go to the Road Haulage Association's Security Audit Service website

**4.1 Social Media**

Posting information can put your personal safety at risk. If you provide too much information and do not have the appropriate privacy settings applied, your business or social network accounts can be a veritable 'gold mine' for those intent on building up a picture of your travel plans, business and other subjects that they may seek to exploit in the future.

Internet-based social networking sites such as Facebook, Twitter, LinkedIn and Instagram are popular applications that allow individuals to create a profile containing personal information and interact with other users. Review your privacy settings otherwise some or all of your on-line social media profiles can be seen by a large audience.

Drivers and passengers should consider if it is appropriate to provide 'live time' information about their activity that would allow them to be targeted. If required, it is always better to post information after the activity has taken place.

Location-based information can be posted on social networks, especially from GPS-enabled mobile devices, which tells others exactly where you are or have been. This information is not secure and could be viewed by anyone, including those who may want to harm you or your family, friends and colleagues. The responsibility rests with you to ensure that no-one is put at risk due to what is disclosed.

Go to the Get Safe Online website

**4.2 Drivers should always**

- Lock and secure their vehicle whenever they leave the cab and, keep the keys with them (including when unloading and loading).
- If possible always refuel on site before beginning a journey.
- Plan routes before beginning a journey.
- Avoid taking the same routes or stops for breaks. These routines make vehicles an easier target for those with criminal intent or conducting hostile reconnaissance.
- Comply with procedures to authorise changes to a delivery destination.
- Never pick up unauthorised passengers/hitch hikers.
- Report any irregularity in loading, locking, sealing or documentation.
- Check their vehicle is correctly loaded.
- Protect documents such as shipping orders and consignment notes. These can be used by criminals to steal valuable loads.
- Avoid talking about loads or routes with other drivers or customers (including over radios and telephones).
- Report suspicious behaviour.

In an emergency call 999

For a non-emergency call 101

If you suspect it, report it to the Anti-terrorist Hotline on 0800 789 321

© NaCTSO Crown copyright 2017

## 5. SECURE WORKING PRACTICES

Security culture must be part of everyone's daily working practice. Businesses should restrict knowledge of loads and routes to those who need to know. The pre-loading of vehicles, should be kept to a minimum. Avoid loading on a Friday afternoon for a Monday morning departure. When pre-loading is necessary, always keep the vehicle on secure premises. If the driver keeps the keys to their vehicle when they are not at work, advise them to:

- keep them secure at all times
- never leave them where they can be copied
- ensure that the keys do not obviously identify the vehicle.

If vehicle keys are kept at the operating centre:

- identify keys control and security measures for vehicles and premises
- keep them in a secure and locked location, out of sight and reach of strangers
- never use a hiding place such as a wheel arch or a peg system that identifies the vehicle.

Be alert to any visual changes to your vehicle. If you notice a suspicious object on or near the vehicle, do not approach or enter the vehicle. Contact the police and give them the location and registration number of your vehicle.

## 6. OVERNIGHT PARKING

Make sure you know where your drivers are parking overnight. Instruct drivers to use pre-planned overnight parking facilities, particularly those that are members of the police Safer Parking Scheme.

The Highways Agency also provides a Truck Stop Guide covering England.

Go to the Safer Parking Scheme website

Go to the Truck Stop Guide

Go to the IRU website

## 7. DRIVER CONTACT

Keep in regular contact with drivers to identify/confirm routes, stops and estimated times of arrival. Drivers should notify employers of changes of routes or unplanned stops.

Go to the Road Haulage Association Security Audit Service website

## 8. PROTEST AT PREMISES OR TOWARDS DRIVERS

It is possible that a company's business association with an organisation could lead to individuals gathering and protesting at your premises or premises to which you make deliveries. Protesters may assemble close to the boundary of the work place or target staff and vehicles.

If this happens:

- Stay calm, individuals may intimidate, but this will not necessarily lead to a physical threat.
- Remain in your vehicle or in the property. Close and lock doors and windows and draw the curtains blinds to premises and vehicles as appropriate.
- Inform the police immediately calling 999 and await their arrival.
- Inform your workplace/colleagues.
- Do not, in any way, respond to, or antagonise, those protesting. Avoid confrontation.
- If someone attempts to confront you, stay in your vehicle. Keep the engine running and if you need to (and it is safe to do so), reverse to get away.
- If possible, note descriptions of individuals and vehicles present.
- If you have a CCTV system fitted that has recorded images, you should hand footage over to the police; it may assist with identification or evidence, where offences are committed.
- Postpone any expected visitors to your site.
- Know exactly where the perimeter of your site is should there be a demonstration.

© NaCTSO Crown copyright 2017

**8.1 If you think you are being followed in your vehicle:**

- Try to stay calm.
- Keep the vehicle moving, even if only slowly.
- Close all windows and ensure the cab is secure.
- Contact the police immediately calling 999.
- If you can, make your way towards the nearest open police station.
- Record the registration number of any suspicious vehicle.

## 9. VULNERABLE/DANGEROUS LOADS

Operators should alert drivers to vulnerable loads or high-consequence dangerous goods and issue them with a vulnerable load/high-consequence dangerous goods card for these loads.

If a vehicle is stopped by uniformed officers in a marked police vehicle or Driver and Vehicle Standards Agency (DVSA) officers, drivers should display the card and follow the instructions on the reverse of the card to verify the identity of officers from the police and DVSA.

During security alerts, operators and drivers should follow the advice given to them by their local police force. (Keep up to date using news media, the MI5 website and relevant associations).

## 10. SECURE VEHICLES

Remember vehicles can be stolen, whatever their load might be, to be used for criminal, including terrorist purposes.

Use and maintain security equipment as it will make your vehicles less attractive to thieves. Discuss options with your insurers, including goods in transit insurers, vehicle dealers and security equipment manufacturers.

- each vehicle will need different levels and types of security equipment, depending on its use
- install vehicle immobilisation, if not already fitted by the manufacturer
- consider the use of telematics equipment which can remotely trigger an alert if a vehicle deviates from its intended route

Contact your local police crime prevention officer and insurer for specific security advice

Go to the Sold Secure website

## 11. PREMISES SECURITY

A third of stolen trucks are taken from the owners' premises, which is why premises security is vital. Consider the following areas when planning your security:

- perimeter protection (fences)
- site access and its control (gates)
- surveillance (lighting and effective CCTV)
- guards
- intruder detection
- visitor control
- limiting the number of key holders
- vehicle key storage
- controlled access to loading bays and control systems
- personnel and vehicle search procedures
- always make sure that any tools or equipment that may help criminals to steal trucks or loads are securely locked away when not in use

## 12. ROOF MARKINGS

The National Police Chief Council (NPCC) has approved the wider use of roof markings on HGVs, to help police air support units to identify vehicles if they are stolen. HGVs, particularly those that regularly carry vulnerable or dangerous loads, should use roof markings.

Go to the NPCC website

## 13. INTERNATIONAL HAULIERS

When travelling abroad all hauliers, drivers and operate should have effective systems to protect their vehicle. Following a simple vehicle security checklist and securing your vehicle reduces delays and possible penalties. Simple steps can make a difference.

You should always:

- Get a checklist and vehicle security instructions from your employer.
- If possible, watch the vehicle being loaded to ensure that no one enters who should not.

© NaCTSO Crown copyright 2017

- Secure your load with a tilt cord and use strong padlocks or seals for load doors and panniers. (They can be glued or pinned together to show they have not been tampered with).
- Check the wind deflector and axles.
- Check the seals, fabric, roof and security devices of the vehicle for damage. If there is evidence of damage or tampering check the load and load space and re-apply security devices. Record the checks made on the checklist, at loading, after every stop and before arriving at the border.

**Be vigilant and speak to a UK Border Agency officer or the police if you suspect that someone has entered or tampered with your vehicle.**

Go to the Government vehicle security checklist

## 14. PREVENTION OF ILLEGAL IMMIGRATION

People attempting to gain illegal entry to the UK will look for HGVs etc. which they believe are heading for the UK. An effective way to deter people is to park facing away from the port, on the other side of the road. This gives the appearance the vehicle is travelling away from the UK and will therefore be less appealing.

To reduce the risk of delay and a possible penalty from the UK Border Agency, make sure that you read and follow the guidance contained in these UK Border Agency documents:

Go to the Civil penalty code of practice: prevention of clandestine entrants

Go to the How to Avoid a Penalty: 10 step guidance for drivers

Go to the Secure, Check, Record vehicle security checklist



© NaCTSO Crown copyright 2017

# Personal security

## 1. PROTECTING YOURSELF AND YOUR FAMILY

Our own security, and the safety of those close to us is of utmost importance. The more you do to protect yourself, the safer you and your family will be. There are three key areas which can affect your safety. These are physical security, situational awareness/security, and online security. This document does not provide definitive advice in all of these areas, but instead provides general guidance along with links to more detailed security guidance, which you may wish to read.

### 1.1 Assessing an appropriate level of protection

This guide provides generic advice on how to stay safe at home, at work, on-the-move, and online. Exactly which measures you adopt will depend on the extent, or level of threat you are likely to encounter and the vulnerabilities you have.

**To help assess this you should consider the following:**

- Your profession/role – does the role you perform make you an attractive target?
- Specific threats – is there credible intelligence to suggest you are at risk?
- Your personal history – have you been targeted in the past?

No-one has more responsibility for your personal security than you. Today individuals face a range of potential threats – from criminals to extremists. Good personal security should take into account both your work and home life and any measures you take should be appropriate to the perceived threat. If they are excessive, they may cause unnecessary inconvenience and stress; if they are insufficient, you may put yourself at risk.

This guidance will help you decide where you need to take precautions, when to maintain heightened awareness and when you should involve the police. No one can be on high alert all the time but do not make their job easier through complacency.

Here are some effective measures you can take. This list is not exhaustive and the precautions you use will depend on individual circumstances.

### 1.2 Vulnerability means there is a risk of successful attack

It is important you learn to recognise situations where you are vulnerable so you can avoid them or, if this is not possible, how to be on your guard. Attackers can be creative when it comes to finding ways and means to target individuals and their families. Their objective may be to cause embarrassment, inconvenience and distress, but may also include the intent to cause physical injury or threaten life itself.

## 2. PHYSICAL SECURITY

### 2.1 Security at home – House and grounds, doors, windows, locks, keys, alarms, lights, CCTV, visitors confidential waste.

There are a number of simple measures you should consider to protect yourself and ensure your home is secure. Protection starts with the perimeter of your property and any fences or walls should be well maintained. It is important that boundaries clearly define the difference between public and private space. Ensure tools and ladders, which could be used to access your home, are locked away and remove anything that could potentially be used to cause damage, such as loose bricks, large stones and garden ornaments.

Make sure good quality locks are fitted to external doors and windows. Remember to keep house keys out of sight, but in a secure place in case of fire. Do not label your keys, if you need to identify keys use a colour-code theme. If you cannot account for all your keys, change the locks.

If you have an alarm installed, you should select an installer who is affiliated to one of the recognised alarm inspectorate bodies, such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB). A monitored alarm may be more expensive but it will cause a response to be undertaken by the alarm company, whereas a purely audible alarm relies on neighbours and passers-by to react.

© NaCTSO Crown copyright 2017

You should make sure you have good external lighting covering external doors, car parking areas and footpaths leading to your home. Consideration should be given to the fitting of floodlights at strategic points to make it difficult for would-be assailants to hide from view. If you consider installing CCTV, seek advice from a professional CCTV installer accredited to one of the recognised CCTV inspectorate bodies, such as the National Security Inspectorate or the Security Systems and Alarms Inspection Board.

If you cannot park your car in a locked garage or a secure parking area then leave your vehicle where it can be seen by the general public. Try to park in a well-lit area, within view of a CCTV camera or in a staffed car park. Always make sure the windows are closed and the car is fully locked and secure.

Go to the Secured by Design website

## 3. SITUATIONAL AWARENESS/SECURITY

### 3.1 Weapons and firearms attacks

The UK government gives some simple actions to consider in the event of a weapons or firearms attack, along with the information that armed officers may need when dealing with such an incident.

Go to the Government's Recognising the terrorist threat webpage

### 3.2 Visitors

Always clearly identify callers to your home before letting them in, and check the identity of tradespeople on their arrival. Never leave them alone in the house. Teach children never to answer the door or let strangers in to your home and tell them to fetch an adult to do it.

### 3.3 Confidential waste

Always treat sensitive, confidential or personal material you are disposing of as confidential waste. Shred it and/or burn it. If shredded at work, put it in a confidential waste bag and keep it safe, not in a public area, until it can be disposed of correctly.

### 3.4 Street safety

Personal safety should always be a key consideration when travelling. By taking suitable precautions you can reduce the opportunity, and therefore the risk, of experiencing violence or aggression. Consider simple measures such as planning ahead before you go out, taking the safest route, and avoiding danger points like quiet or poorly lit alleyways or isolated car parks.

When out, if you are at all worried, try and stay near a group of people. Whenever possible, walk facing oncoming traffic to avoid vehicles approaching from behind you. Never accept a lift from a stranger or someone you don't know well, even if the weather is poor or you're late. Keep your mind on your surroundings – if you are talking on your phone or wearing headphones, you will not be aware of potential problems near you. Be particularly careful when using cash machines. Make sure nobody is loitering nearby and do not count your money in the middle of the street. Consider carrying a personal safety alarm, which can be used to disorientate an attacker giving you vital seconds to get away.

Go to the Suzy Lamplugh Trust website

### 3.5 Meetings and surgeries

If you are an MP, Councillor or a GP for example, you will have to conduct meetings or surgeries. You may be alone in an office or meet people who are confrontational or in different states of distress. They may display different emotions and be upset, angry or aggressive. It is important to continually assess your surroundings, the person's behaviour and potential threats before and during meetings. You should take proportionate steps to reduce the risks and stay safe.

### 3.6 Motor vehicles and travel

If possible avoid setting patterns in your travel arrangements which could make it easy for anyone to predict your whereabouts. Vary your routes and times of departure as much as possible. Lock the vehicle doors and boot during your journey. Open windows only enough for ventilation purposes, particularly in town. Keep your

© NaCTSO Crown copyright 2017

distance from the vehicle in front. You should always check you have the fuel required to complete your journey.

If you break down on a motorway, it is usually safer to wait for assistance outside your vehicle, standing on the verge or behind the crash barrier. Take your keys with you and lock all doors except the one nearest to you, which you can leave wide open so that you can get in quickly if you need to. Make a habit of checking the road before leaving your home or place of work. Note and report any suspicious or strange vehicles.

If you think you are being followed, try to remain calm and keep your vehicle moving, even if only slowly. Close all windows and ensure that your doors and boot are locked. Contact the police immediately. If you can, make your way towards the nearest open police station. Do not drive home. Record the registration number of any suspicious vehicle.

### 3.7 Anonymous telephone calls and threats

These are usually intended to cause fear, alarm and distress. These calls can be extremely distressing but, if it is bearable, keeping the caller talking can reveal important information. It is a criminal offence to make threatening or abusive telephone calls and you should consider contacting the police.

Go to the Ofcom Abusive and threatening calls webpage

Go to the Ask the Police website

## 4. ONLINE SECURITY

### 4.1 Use of mobile devices

Mobile devices can hold a variety of personal details such as online banking, emails, diary, contacts, social media and photographs. To keep your device secure you should use all it's security features. These include setting up device tracking and creating screen and SIM pass codes. Switch off GPS tracking when it is not required.

An IMEI is a unique 15 digit serial number which can be used to identify a lost or stolen phone or mobile enabled tablet. Keep a record of your device's IMEI number. IMEI number can be on the back of a device, under a removable battery or on the device's original packaging. You can also get it by typing *#06# into your phone.

Always change the default PIN for voicemail access. Avoid using public Wi-Fi hotspots as they may not be secure. You should consider disabling location services on your phone, if appropriate, and review privacy settings to prevent someone tracking your movements and identifying your home address or place of work. Geotagging marks a video, photo or other media with a location which can reveal private information to a third party. Remove metadata from pictures, especially ones taken from mobile phones before you post them online.

### 4.2 Safely using the internet and managing personal information online

The internet can be a valuable source of information, education and entertainment. However, you should take precautions online with the amount of personal information you publish, especially for social networking purposes.

### 4.3 Online Social Networking (OSN)

Popular sites, such as Facebook, Twitter and Instagram, allow individuals to create a personal profile and interact with other users online. Additionally business networking sites, such as LinkedIn, also require personal profiles to include an individual's work history.

Whilst these are useful tools to communicate with others or advertise your professional skills, publishing personal information online presents potential risks.

You may be susceptible to identity theft as dates of birth, full names, home addresses and email details are key pieces of information for identity fraudsters. In addition, information regarding employment, personal or work addresses, family members, hobbies or vehicle details are also extremely valuable to criminals and other potentially hostile parties. Some social networking sites own any data posted on them and may reserve the right to sell your details to third parties.

You should regularly review your privacy settings for these sites otherwise some or all of your personal profiles could be seen by a large audience unknown to you. Additionally,

© NaCTSO Crown copyright 2017

your family and friends can innocently divulge information about you if they do not take appropriate measures to protect their profile information.

**4.4 Doxing**

Doxing is the practice of researching and publishing private or identifying information about a particular individual on the internet. Online research is used by a wide group of terrorists and hacktivists alike to harvest information on individuals. This can then be used to incite fear in target populations and individuals, and therefore satisfies some terrorist objectives.

Posting information online can put your personal safety at risk. If you provide too much information and do not have the appropriate privacy settings applied, your business or social network accounts can provide a lot of useful information for those intent on building up a picture of your relationships, opinions, places of interest and any other subject that they may seek to exploit in the future.

Location-based information can be posted on social networks, especially from GPS-enabled mobile devices, which tells others exactly where you are or have been. This information is not secure and could be viewed by anyone, including those who may want to harm you or your family, friends and colleagues. The responsibility rests with you to ensure that no-one is put at risk due to what is disclosed.

Go to the National Cyber Security Centre website

## 5. DEMONSTRATIONS

It is possible that your profession or association with an organisation could lead to protesters gathering at your home or work. They may assemble close to the boundary of your home, work place or even on your property. If this happens, stay calm – such protests may intimidate but will not necessarily lead to a physical threat. Remain inside, close and lock doors and windows and draw curtains/ blinds. Call the police on 999. If possible, note descriptions of individuals and vehicles present. If you have a CCTV system fitted that has recorded images of protesters, you should hand any footage obtained over to the police; it may assist with identification and provide evidence in cases where offences have been committed.

**GO TO SECTION CONTENTS**

You may also want to read A Guide to Personal Security: published by NaCTSO, it is available through your local CTSA

Go to the CPNI website

Go to the Get Safe Online website

Go to the Cyber Streetwise website

Go to the CPNI Employee Digital Footprint campaign webpage

Go to Glossary

© NaCTSO Crown copyright 2017

# Overseas travel advice

## 1. INTRODUCTION: GUIDANCE FOR THE ORGANISATION

Organisations have a duty of care towards those who travel overseas for work purposes. By having the right security policies and procedures in place an organisation will be better prepared to support their traveller should a security situation, such as a terrorist incident, occur.

The organisation also has the opportunity to equip their travellers with the security knowledge and behaviours that they need to help keep themselves secure while travelling overseas.

This guidance has been designed to support organisations in understanding how they are able to mitigate risk to their employees and respond effectively to situations as they arise. The guidance also contains tips for organisations to communicate travel security messages to their employees, so that they too take responsibility for their travel security.

### 1.1 Risk Assessment

Ensure that the travel is necessary for the organisation's purposes. Are there other, lower risk ways of meeting the business objective e.g. through video conferencing. Carry out an up-to-date risk assessment of the destination and the proposed travel itinerary. Appraise the risk from a range of threats which will include terrorism amongst others e.g. criminality, espionage, environmental disasters. Use authoritative sources of information such as the Foreign & Commonwealth Office foreign travel advice website to inform the assessment.

Go to the FCO travel advice website

### 1.2 Educating travellers

Where appropriate, provide security briefings for travellers that are tailored and relevant to their destination. Appraise travellers of the threats at their destination but avoid focusing too heavily on this as it can overwhelm them. They should leave the briefing with an understanding of the important role that they can play in keeping themselves secure.

Ensure that employees are aware of the support that the organisation provides for travellers e.g. security advice, travel healthcare arrangements and what they should do in an emergency. Travellers may require other relevant security information e.g. an understanding of how to manage their online profile as this is central to their ability to keep a low profile when overseas.

### 1.3 Travel booking procedure

Procure travel and accommodation services through a reputable company. If your organisation allows employees to book their own travel make sure that the proposed airlines and travel providers have a good track record on safety and security.

Think about how you may be able to access your in-house travel bookings to see details of who is scheduled to be at a particular destination and when. Having accurate information such as this is vital for your organisation to provide an effective, timely response in an emerging crisis.

### 1.4 Maintaining contact with the traveller

Ensure that you have reliable systems in place to remain in touch with your employees when overseas.

Provide an emergency point of contact that is available to the traveller 24/7 while overseas. Use an accessible format, such as providing a wallet card, so that the traveller is more likely to have your contact details with them overseas.

Ensure that there is an accessible record within the organisation of the detailed itinerary of the traveller. Encourage the traveller to check-in with the organisation at regular points and if their travel plans change.

It is good practice to have an emergency point of contact for the traveller's home life, to ensure smooth communication should an incident arise.

Consider providing the traveller with a mobile phone that will work at their overseas destination to ease communication.

© NaCTSO Crown copyright 2017

**1.5 Emergency provisions**

Prepare a proportionate risk-management and contingency plan that includes how to respond should the traveller be involved in a security incident overseas.

Ensure that your organisation has a procedure in place for staying up-to-date with emerging security issues that may be relevant to overseas travellers, using trusted, new sources. Have clearly identified roles and a chain of responsibility in case of a terrorist incident, ensuing there is someone available and able to make decisions to support travellers, such as accessing funds in an emergency.

Consider using medical and travel security assistance providers who can provide 24 hour services and advice in an emergency to travellers e.g. via specialised mobile applications or messaging services.

**1.6 Debriefing travellers**

Ensure that you have appropriate systems and services in place to support travellers upon their return, especially if they have been involved in an incident whilst overseas.

Give travellers an opportunity to provide feedback on their recent trip as this is an important way of ensuring your travel policies and procedures remain fit-for-purpose for travellers.

**1.7 Tips for communicating travel security messages to travellers**

- Ensure that your organisation's travel security policies and procedures are straightforward and easy to find to maximise the chances that travellers can follow the intended process.
- Preparing for an overseas work trip is a very busy time, make it easier for your travellers to follow security advice by sticking to a manageable number of key security principles.
- Ensure that travellers are clear about the behaviours you expect of them when they are overseas and that they understand why these will help to keep them safe.
- Aim to use case-studies and examples to bring the threat to life so that travellers understand the context of the security advice that you are delivering.
- Foster a sense of responsibility on the part of the traveller. Although the organisation will have certain protections in place, it is the traveller who will need to behave securely while they are overseas. Personal security is a personal responsibility.
- Provide security messages in accessible formats to travellers. Think about whether security advice can be integrated into the travel booking process e.g. at briefings, when booking travel etc.
- Make the security messages relevant for travellers in their personal lives to increase engagement with the security advice.

## 2. GUIDANCE FOR THE TRAVELLER

The following security advice has been provided to help you to communicate your key security messages to your travellers:

"The chances of being caught up in a terrorist incident are low. But when travelling overseas the security situation on the ground can change rapidly and unexpectedly. As a traveller you may be less familiar with how to behave should an incident occur, than you would be if you were in the UK. There are important practical steps that you can take to reduce the likelihood of being directly involved in a terrorist incident and to be best prepared should a situation arise. The security advice provided here has been designed for those who travel overseas for work purposes. You may also find these tips helpful to keep you and your co-travellers safe during your own personal travel."

**2.1 Before you travel**

- Use authoritative sources such as the Foreign & Commonwealth Office website to check the latest advice for your destination.
- Avoid mentioning that you are travelling or providing details of your trip online (including on social media). This will prevent others from having the opportunity to plan to target you when overseas.
- Choose your travel route to avoid additional security risk. Can you avoid a stop-over in a high risk country? Does your airline/travel provider have a good reputation for safety and security?

© NaCTSO Crown copyright 2017

- Think about whether your plans involve arriving at your destination late at night or early in the morning. If so, what onwards transport options will be available to you?
- Have an emergency contact at home and share a detailed itinerary with them so that someone knows where you are in case of emergency. If you are travelling for work purposes, make sure that you arrange for the same with your organisation.
- Make copies of your passport and travel documents and keep these separate. This will make the process of applying for replacements easier if required.
- Ensure that you have appropriate health insurance coverage. Share the details with your emergency contacts and take a copy with you overseas.
- Take a mobile phone with details for your emergency contacts at home and within your destination country. Would you know how to contact the emergency services if an incident occurred?
- Where possible do not take expensive items with you (e.g. jewellery, designer clothing, and unnecessary electronic devices) as they may make you appear to be an attractive target to criminals and others with hostile intent.

Go to the FCO travel advice website

**2.2 While travelling**

- Keep a charged mobile phone with you so that you are contactable in an emergency. Consider taking a portable battery charger with you to ensure you remain contactable.
- Keep an eye on local sources of news to ensure you are aware of any developing situations that could impact your personal security.
- Keep your points of contact up-to-date if your travel plans change.
- Maintain awareness of your surroundings; avoid distractions such as using headphones as they will slow your reaction if a threatening scenario emerges. Appearing alert will also help you to look like a harder target to deter potential attackers and criminals.
- Look out for those acting suspiciously and for unattended items such as bags and packages. If something doesn't feel right, trust your instincts and report it to a security guard or law enforcement official as soon as you can.
- Avoid setting patterns in your day-to-day activity that could be used to target you. Vary timings, modes of transport and routes where possible.
- Be wary of those showing you undue attention and asking a lot of questions that are personal in nature.
- Try to minimise the time you spend in public areas within airports. At your earliest convenience, move through security to a safer area.
- Where possible, avoid crowded situations where you may stand out or be targeted as a foreigner e.g. protests and other civil unrest scenarios.
- Avoid styles of dress and personal behaviour that may draw attention to yourself.
- Use only licenced vehicles.
- Where possible avoid walking alone at night.
- If driving overseas, make sure that your vehicle is in good working condition before starting each journey and there are no signs of tampering. While driving make sure windows and doors are locked.
- Be sure of the identity of visitors before opening your hotel room door; use security chains and locks as appropriate when you are inside your room.
- Refuse to accept unexpected packages.
- Consider utilising a door jammer or door wedge.
- Identify potential emergency exits and routes to safety so that you will be prepared if a situation arises.

Familiarise yourself with the latest guidance on how to behave if you become involved in a terrorist incident:

**RUN** to a place of safety, if you can't do this,
**HIDE** turn your phone to silent and barricade yourself in if possible.
**TELL** call the police when it is safe for you to do so.

© NaCTSO Crown copyright 2017

**2.3 When you return**

Let your emergency points of contact know that you have returned safely. If you are travelling for work purposes your organisation may be interested in any feedback you may have to help to improve security advice for future travellers. Report any suspicious incidents that occurred overseas.

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Cyber security

## 1. INTRODUCTION

Many organisations rely upon information systems to carry out business or nationally critical functions and employ digital technologies to manage safety, security and engineering systems. As a result they can become vulnerable to threats related to the control of access to and operation of their systems, compromise of information quality or validity, and loss of information or system availability. The consequences of such incidents can be critical to the organisation, leading to loss of reputation, damage to assets or result in serious injury or fatalities.

Your sensitive information may be of interest to business competitors, criminals, foreign intelligence services or terrorists. They may attempt to access this 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 measures, you should assess the risks posed to your organisation by considering what assets and key information or datasets you have, what or who poses a threat to you and how, and what vulnerabilities you have in your systems and processes. The key questions for you to consider are:

- 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, your customers or partners?
- Who has access to your sensitive information within your organisation, in your supply chain, and in other organisations, e.g. local authorities and regulators?
- Consider current good practice information security for countering electronic attack and for protecting documents.

Go to the NCSC guidance webpage

### 1.1 Cyber attacks

The internet is a great business enabler and a fully established part of our working and home lives, but it is important to be mindful of the fact that when you entrust your information or business processes to a computer system, they are at risk. Cyber attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet. This interconnectivity has become increasingly common.

Cyber attacks could:

- Allow the attacker to gain access to your computer system and do whatever the system users, administrator or owner can do, e.g. take control of a physical system or make unauthorised transactions.
- Steal or modify your data, perhaps subtly so that it is not immediately apparent.
- Install malicious software, e.g. ransomware or to maintain unauthorised access.
- Overwhelm your system by flooding its servers with unwanted data making it impossible to use, resulting in your customers being unable to access your website and online services; this is known as a Distributed Denial of Service (DDoS) attack and can be difficult to protect against.

### 1.2 Malicious software

The techniques and effects of malicious software (e.g. malware such as viruses, worms, and trojans) are as variable as they are widely known. The main ways that malware can spread are through:

- Running or executing an attachment received in an email, or clicking on a website link.
- Browsing illegal or unfamiliar websites, which can result in the distribution of malicious software, sometimes referred to as a ‘drive-by’ attack.
- Allowing staff to connect removable media, e.g. USB memory sticks, CDs, media players, mobile phones and chargers to corporate machines or devices; USB connections are a common way to infect devices and can even be used to launch attacks on your home and/or corporate network.

### 1.3 Malicious software – preventative measures

The preventative measures below are applicable for both corporate and personal IT security:

- Use a firewall and anti-virus software and keep them up to date; run regular system scans.

© NaCTSO Crown copyright 2017

- Use applications from reputable sources and avoid using third party applications.
- Malware can spread rapidly via email and other methods; do not open emails from unknown or suspicious senders.
- Treat all email attachments and links from unknown or unfamiliar senders with caution as this may be a phishing attack (see 1.5).
- Use software controls that ensure only trusted websites can be accessed, reducing the risk of malicious software being installed on your system.
- Issue guidance and educate your staff to ensure compliance.
- Implement an 'acceptable use policy' for staff concerning web browsing, email, use of chat rooms, social networking, trading, games and music download sites etc.
- avoid downloading files from illegal sharing sites as there is an increased risk of malware infection.
- Instead of using removable media to store or move files, use secure cloud storage solutions that have been approved by your organisation.
- Use a second mains charger to reduce the temptation of charging mobile devices using an unmanaged source.

Go to the NCSC Cloud security guidance

**1.4 Passwords**

Passwords protect important information and when implemented correctly are a free, easy and effective way to prevent unauthorised users accessing your devices. Never use the same password at work that you use when at home. Your password should be easy for you to remember, but hard for somebody else to guess. A good rule is make sure that somebody who knows you well couldn't guess your password in 20 attempts:

- Use strong passwords that do not feature familiar words and avoid using the same password across systems and applications.
- If you must write down passwords to prompt memory, ensure they are properly secured, e.g. locked cabinet, but never in the same place as the device.

Go to the NCSC Password guidance

**1.5 Phishing attacks**

Phishing is a particular type of email scam. During a phishing attack, attackers send mass emails- seemingly from genuine people or services- to hundreds of thousands of recipients, asking for sensitive information or encouraging them to visit a fake website.

Example of phishing attacks include:

- An email claiming to be from a bank or website where you have an account, requesting you log in to verify your account due to fraudulent activity that has taken place; the email would normally include a link that directs you to a website that looks similar to the genuine banking site, but is instead logging any details you type in.
- An email stating you've been charged for a service that you didn't use with an attached document that is supposed to be an invoice; when the attachment is opened, a malicious program is automatically installed on your computer without your knowledge.

**1.6 Spear-phishing**

Spear-phishing is a more targeted form of phishing. During a spear-phishing attack the email is often directed at specific people and designed to look like it's from a person the recipient knows or trusts. An example of this would be an email that appears to come from a senior person within your own organisation requesting a payment is made to a particular bank account or requesting that you forward some sensitive information or documents.

## 2. IT SECURITY AND ONLINE COMMUNICATIONS

Mobile technology is now an essential part of modern business, with more of our data being stored on tablets and smartphones. What's more, smartphones and tablets are now as powerful as traditional computers and because they often leave the safety of your office and home they need even more protection than desktop equipment. They're also frequently connected to public Wi-Fi, which introduces further security issues. It is important to follow a few basic steps to keep your mobile devices and the information stored on them secure.

© NaCTSO Crown copyright 2017

If you or your company are about to invest in a new device, it is recommended that you read the Buyer's Guide to Choosing and Using Mobile Devices produced by the Home Office.

Go to the Buyer's Guide to Choosing and Using Mobile Devices

Think about the activities you use your device for – online banking, personal and work emails, social media and photographs. Do you want these to be made public or used against you? Be mindful that location services can potentially allow someone to track your movements and ultimately reveal your home address and place of work. Geo-tagging marks a video, photo or other media, and postings such as tweets with a location and this can reveal private information to a third party. You should balance risk versus usability depending on your personal and corporate needs:

- Use all of the security features available, e.g. device tracking, screen and SIM passcodes.
- Consider 'safe loss' and remote lock or wipe options in the event your device is lost or stolen.
- Retrieve your data from an automatic backup of the device while keeping this data safe from attackers.
- For organisations, enabling these features across your entire workforce may seem daunting but mobile device management software allows you to set up your devices to a standard configuration with a single click.
- Record the IMEI numbers for your phone and tablet; an IMEI is 15 numbers long and uniquely identifies your phone and can be found on the phone box package, under the phone battery or found by typing *#06# into your phone.
- Change the default PIN for voicemail access.
- Avoid using public Wi-Fi hotspots (hotels, coffee shops) as these may not be secure allowing a 3rd party to access your sensitive data; instead use inbuilt security within 3G/4G networks or use Virtual Private Networks (VPNs) so that your data is encrypted before being sent.
- Regularly review your privacy settings, particularly after software or operating system upgrades, and when you install new software or applications.

## 3. MALICIOUS MODIFICATION OF HARDWARE

Computer hardware can be modified to mount or permit an electronic attack. This can be done at the point of manufacture or supply, prior to installation, during maintenance visits, when off-site for repair or by an insider. However, this threat also extends to anyone who has physical access to your hardware. The purpose of such modifications would be to allow a subsequent attack to be made, possibly by remote activation. What to do:

- Acquire your IT devices, equipment and systems from reputable manufacturers and suppliers.
- Ensure that your software is regularly updated by trusted partners; reputable suppliers are continually fixing security vulnerabilities in their software via patches available from their websites.
- Configure your operating system and application software so that is checks for patches and downloads updates at least weekly and enable auto-update options.
- Ensure that all your computer hardware is equipped with anti-virus software and is protected by a firewall.
- Back up your information, preferably in an alternative secure location e.g. encrypted cloud storage accessed via a secure connection.
- Put in place a framework to assess the reliability of those who maintain, operate and guard your systems, whether employed by you organisation or provided by your supply chain.
- Consider encryption packages for material you want to protect, particularly if taken offsite- but seek expert advice first.
- Encourage security awareness among your staff, including a clear desk policy and locking away mobile devices when not in use.
- Make staff aware of social engineering that can trick users into revealing sensitive information.
- Invest in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material, both printed and digital media.

© NaCTSO Crown copyright 2017

## 4. THE INSIDER THREAT

The cyber threat to your organisation is most likely to come from an external source; however, it is crucial that you also consider the threat posed to your information and systems from individuals with legitimate access to your premises and networks. Insider risks are becoming more prominent and the potential for trusted users to steal large amounts of information is increasing, as computing and storage increases; as the Edward Snowden case showed. Insider risks are as much a Personnel Security problem as they are for those responsible for physical and IT security. The security communities within your organisation should work together to address them. It is essential that you maintain accurate records of all staff with access to your systems and have in place effective security policies and the means of auditing staff IT use.

Consider the points below as part of effective governance, risk and compliance (GRC) approach:

- Ensure each individual's physical, information and system access is appropriate to their role.
- Ensure system administrator rights are limited to those people who actually need it and that the individuals use a separate lower privilege account for routine activities, e.g. email and web browsing.
- Have in place an effective exit procedure to ensure former employees no longer maintain any system access and that the reason for leaving are understood.
- Ensure that your human resources department always calls your IT staff when an employee leaves your organisation, or when they are investigated for poor performance or bad behaviour.
- Ensure policy adequately covers the insider threat and investigation protocols are clearly understood by all those involved.
- Ensure that your IT systems have controls in place to prevent certain user acts that might result in information theft or other compromises, e.g. control of USB devices, blocking internet access to inappropriate websites, read/write privileges.
- Ensure that user activities on IT can be monitored for prohibited or suspicious acts; maintaining appropriate system access logs is essential if digital forensics are to be effectively used to investigate serious security breaches.

## 5. CYBER ESSENTIALS

Cyber Essentials is a new government-backed and industry-supported scheme to guide organisations in protecting themselves against cyber threats. The Cyber Essentials scheme provides businesses small and large with clarity on good basic cyber security practice. By focussing on basic cyber hygiene, your company will be better protected from the most common cyber threats. Cyber Essentials is for all organisations, of all sizes, in all sectors.

Go to the Cyber Essentials webpage

## 6. THE 10 STEPS TO CYBER SECURITY

For organisations facing a higher level of cyber security threat the Government recommends employing the 10 steps to cyber security, which are listed on the next page.

**GO TO SECTION CONTENTS**

Go to the CPNI website

Go to the Cyber Aware website

Go to the NaCTSO website

Go to the National Cyber Security Centre website

Go to the Register of Security Engineers and Specialists website

Go to Glossary

© NaCTSO Crown copyright 2017

## 10 STEPS TO CYBER SECURITY

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

**Network Security**
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

**User education and awareness**
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

**Malware prevention**
Produce relevant policies and establish anti-malware defences across your organisation.

**Removable media controls**
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

**Secure configuration**
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

**Managing user privileges**
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

**Incident management**
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

**Monitoring**
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

**Home and mobile working**
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

© NaCTSO Crown copyright 2017

# Personnel security

Identity assurance

| **During recruitment you should require** | Yes | No | Unsure |
|---|---|---|---|
| Full name | ☐ | ☐ | ☐ |
| Current address and any previous address in the last five years | ☐ | ☐ | ☐ |
| Date of birth | ☐ | ☐ | ☐ |
| National Insurance number | ☐ | ☐ | ☐ |
| Full details of references (names, addresses and contact details) for both character and employment | ☐ | ☐ | ☐ |
| Full details of previous employers, including dates of employment | ☐ | ☐ | ☐ |
| As a minimum an employer should ask for a self-declaration of criminal record. Advice on how this can be done can be found at: https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf | ☐ | ☐ | ☐ |
| Proof of relevant educational and professional qualifications | ☐ | ☐ | ☐ |
| Financial checks – an employer should consider these checks if they role applied for will have financial responsibilities | ☐ | ☐ | ☐ |
| Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals | ☐ | ☐ | ☐ |
| Consider social media checks, anyone using social media for screening purposes must follow some careful guidelines https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf | ☐ | ☐ | ☐ |

© NaCTSO Crown copyright 2017

| **Do you ask British citizens for** | Yes | No | Unsure |
|---|---|---|---|
| Full (current) 10 year passport | ☐ | ☐ | ☐ |
| British driving licence (photo licence) | ☐ | ☐ | ☐ |
| P45 | ☐ | ☐ | ☐ |
| Birth certificate, issued within six week of birth | ☐ | ☐ | ☐ |
| Credit card, with three statements and proof of signature | ☐ | ☐ | ☐ |
| 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 | ☐ | ☐ | ☐ |
| A Home Office document confirming the individual's UK immigration status and permission to work in the UK | ☐ | ☐ | ☐ |
| Identity Card for foreign nationals. | ☐ | ☐ | ☐ |
| Further information is available at www.gov.uk/identitycards | | | |

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# CCTV

Does your site have a strategic security plan (SSP) developed using an Operational Requirement (OR)?

| | Yes | No | Unsure |
|---|---|---|---|
| Is your control room designed to support the activities of the control room operators and ensure an effective CCTV function? | ☐ | ☐ | ☐ |
| Is your CCTV system designed to protect critical assets against security threats and effective in detecting and investigating crime? | ☐ | ☐ | ☐ |
| Are your CCTV cameras positioned in locations to monitor or detect suspicious activity in areas where hostiles will have to visit to gain the information they need? | ☐ | ☐ | ☐ |
| Do you have CCTV cameras covering critical areas in your business, such as server rooms, back-up generators, cash offices and back of house corridors? | ☐ | ☐ | ☐ |
| Could you positively identify an individual from your recorded images of a hostile? | ☐ | ☐ | ☐ |
| Do the CCTV cameras support your access control systems and cover both vehicle and pedestrian entrances and exits? | ☐ | ☐ | ☐ |
| Have you considered the introduction of ANPR to complement your security operation? | ☐ | ☐ | ☐ |
| Is each CCTV camera doing what it was installed to do? | ☐ | ☐ | ☐ |
| Does the lighting system complement the CCTV system during daytime and darkness hours? | ☐ | ☐ | ☐ |
| Do you constantly monitor your CCTV images or playback overnight recordings for evidence of suspicious activity? | ☐ | ☐ | ☐ |
| Are your 'contracted in' CCTV operators licensed by the Security Industry Authority (SIA)? | ☐ | ☐ | ☐ |
| Does your system comply with the Data Protection Act 1998? | ☐ | ☐ | ☐ |
| Do you store the CCTV images in accordance with the evidential needs of the police? | ☐ | ☐ | ☐ |
| Do you have an emergency callout contract and are your CCTV cameras regularly maintained? | ☐ | ☐ | ☐ |
| Can your control room provide both communications of the threat in advance and effective communication during an attack? | ☐ | ☐ | ☐ |

© NaCTSO Crown copyright 2017

| | | | |
|---|---|---|---|
| Is your CCTV system reviewed regularly as the risks an organisation faces are likely to change over time? | ☐ | ☐ | ☐ |
| Do your systems meet all of the relevant British and European Standards? | ☐ | ☐ | ☐ |

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Access control

| | Yes | No | Unsure |
|---|---|---|---|
| Do you prevent all vehicles from entering adjacent to crowded places until they are authorised by your security? | ☐ | ☐ | ☐ |
| Do you have physical barriers in place to prevent unauthorised vehicles accessing your location? | ☐ | ☐ | ☐ |
| Is there clear demarcation identifying the public and restricted areas of your institution? | ☐ | ☐ | ☐ |
| Do staff, contractors, cleaners and other employees wear ID badges at all times on site? | ☐ | ☐ | ☐ |
| Do you adopt a 'challenge culture' to anybody not wearing a pass in your restricted areas? | ☐ | ☐ | ☐ |
| Do you record details in advance of vehicles, drivers and passengers requiring access to your site? | ☐ | ☐ | ☐ |
| Do you require driver and vehicle details of waste collection services in advance? | ☐ | ☐ | ☐ |
| Do you refuse entrance to unexpected vehicles? | ☐ | ☐ | ☐ |
| Do all visitors in non-public areas have to report to reception before entry? | ☐ | ☐ | ☐ |
| Are visitors required to sign in and issued with a visitors pass? | ☐ | ☐ | ☐ |
| Do visitors' passes look different from staff badges? | ☐ | ☐ | ☐ |
| Are all visitors' passes collected from visitors when they leave? | ☐ | ☐ | ☐ |
| Does a member of staff accompany visitors at all times while in restricted areas of your institution? | ☐ | ☐ | ☐ |
| Do you have CCTV and alarms covering access controlled doors? | ☐ | ☐ | ☐ |
| Is your access control system actively managed? | ☐ | ☐ | ☐ |

© NaCTSO Crown copyright 2017

| | Yes | No | Unsure |
|---|---|---|---|
| Can you use your automatic access control system (AACS) during a lockdown? | ☐ | ☐ | ☐ |
| Can you implement security upgrades during times of increased threat such as search procedures or limiting access to your site? | ☐ | ☐ | ☐ |
| Do you have access control policies and procedures in place? | ☐ | ☐ | ☐ |
| Are your staff trained in your access control policies and procedures? | ☐ | ☐ | ☐ |
| Do you search visitors, customers or contractors? | ☐ | ☐ | ☐ |
| Do you search vehicles before entering the site? | ☐ | ☐ | ☐ |
| Have the staff who search people or vehicles had adequate training? | ☐ | ☐ | ☐ |

Is your access control system compliant with:

| | | | |
|---|---|---|---|
| The Disability Discrimination Act 1995 | ☐ | ☐ | ☐ |
| The Human Rights Act 1998 | ☐ | ☐ | ☐ |
| Health and Safety Acts | ☐ | ☐ | ☐ |
| The Data Protection Act 1998 | ☐ | ☐ | ☐ |
| The Fire Safety Order 2005 | ☐ | ☐ | ☐ |
| The Fire (Scotland) Act 2005 | ☐ | ☐ | ☐ |

| | | | |
|---|---|---|---|
| Are critical areas kept secure during a fire or emergency alarm? | ☐ | ☐ | ☐ |
| Do you vet staff, visitors and contractors before allowing access to restricted areas? | ☐ | ☐ | ☐ |

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Bomb threats

## ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

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

## ASK THESE QUESTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?
2. When is it going to explode?
3. What does it look like?
4. What does the bomb contain?
5. How will it be detonated?
6. Did you place the bomb? If not you, who did?
7. What is your name?
8. What is your address?
9. What is your telephone number?
10. Do you represent a group or are you acting alone?
11. Why have you placed the bomb?

Record time completed:

© NaCTSO Crown copyright 2017

## INFORM BUILDING SECURITY OR COORDINATING MANAGER

Name and telephone number of person informed:

## DIAL 999 AND INFORM POLICE

Time informed:

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

Date and time of call:

Duration of the call:

The telephone number that received the call:

**About the caller:**

☐ Male ☐ Female Age

Nationality

**Threat language:**

☐ Well-spoken ☐ Irrational ☐ Taped

☐ Foul ☐ Incoherent

**Caller's voice**

☐ Calm ☐ Slurred ☐ Lisp ☐ Familiar (If so, who did it sound like?)

☐ Crying ☐ Excited ☐ Rapid

☐ Clearing throat ☐ Stutter ☐ Deep ☐ Accent (If so, what accent?)

☐ Angry ☐ Disguised ☐ Laughter

☐ Nasal ☐ Slow ☐ Hoarse

☐ Other (please specify)

© NaCTSO Crown copyright 2017

**Other sounds:**

| | | | |
|---|---|---|---|
| ☐ Street noises | ☐ Motor | ☐ PA system | ☐ Office machinery |
| ☐ House noises | ☐ Clear | ☐ Booth | ☐ Other (please specify) |
| ☐ Animal noises | ☐ Voice | ☐ Music | |
| ☐ Crockery | ☐ Static | ☐ Factory machinery | |

Remarks

Additional notes:

Signature _____

Print name _____

Date ____ / ____ / _____

© NaCTSO Crown copyright 2017

## ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1. do not reply to, forward or delete the message
2. if sent via email, note the address
3. if sent via social media, what application has been used and what is the username/ID?
4. dial 999 and follow police guidance
5. preserve all web log files for your organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

Signature _____

Print name _____

Date ____ / ____ / _____

## SAVE AND PRINT – HAND COPY TO POLICE AND SECURITY OR COORDINATING MANAGER

Retention period: 7 years

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Emergency and business continuity planning

Business continuity is an essential part of any organisation's response planning. It sets out how the business will operate following an incident and how it expects to return to 'business as usual' in the quickest possible time.

A Business Continuity Plan (BCP) need not be specific to terrorist incidents and applies to any major disruption such as fire, flooding or power fault.

An emergency response plan is a plan of action for the efficient deployment and coordination of services, agencies and personnel to provide the earliest possible response to an emergency.

| | Yes | No | Unsure |
|---|---|---|---|
| Do you have incident reporting and management procedures? | ☐ | ☐ | ☐ |
| Do you review and update your procedures every 6 months? | ☐ | ☐ | ☐ |
| Do you have a risk register that includes all significant risks to the business? | ☐ | ☐ | ☐ |
| Do you review and update your risk register every 6 months? | ☐ | ☐ | ☐ |
| Do you have a Business Continuity Plan (BCP)? | ☐ | ☐ | ☐ |
| Do you have Business Continuity Plans in place to cater for the loss/failure of key sites, systems equipment and personnel? | ☐ | ☐ | ☐ |
| Do you review and update your plans every 6 months? | ☐ | ☐ | ☐ |
| Do you have emergency response plans? | ☐ | ☐ | ☐ |
| Do your emergency response plans include firearms and weapons attacks? | ☐ | ☐ | ☐ |
| Do your emergency response plans include evacuation, invacuation and lockdown procedures? | ☐ | ☐ | ☐ |
| Do you have defined primary and secondary evacuation assembly points? | ☐ | ☐ | ☐ |

© NaCTSO Crown copyright 2017

| | | | |
|---|---|---|---|
| Do you test your primary and secondary evacuation points annually? | ☐ | ☐ | ☐ |
| Do you test your invacuation point annually? | ☐ | ☐ | ☐ |
| Do you exercise your plans at least annually? | ☐ | ☐ | ☐ |
| Are your staff trained in activating and implementing your incident management and BCP? | ☐ | ☐ | ☐ |
| Have you prepared an emergency crisis management kit? (grab bag) | ☐ | ☐ | ☐ |
| Are your emergency crisis management kit (grab bag) contents reviewed every 6 months? | ☐ | ☐ | ☐ |
| Do you have access to an alternative fall back site to use in an emergency? | ☐ | ☐ | ☐ |
| Is your alternate fall back site tested annually? | ☐ | ☐ | ☐ |
| Are your critical documents adequately protected? | ☐ | ☐ | ☐ |
| Do you have copies of your critical documents at a separate location? | ☐ | ☐ | ☐ |
| Are your critical documents available 24/7? | ☐ | ☐ | ☐ |
| Do you have a budget? (Covering the cost of the measures is essential to ensure the continuation of business in every circumstance) | ☐ | ☐ | ☐ |

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# ETHANE

Initial actions at a terrorist major incident:

**Exact location**
- Confirm nearest junction or exact address
- Geographic size of the incident

**Type of incident**
- Explosion, building collapse, firearms incident etc.

**Hazards**
- Identify the hazards present or suspected (e.g. number of hostiles, types of weapons etc.)
- Consider potential or secondary devices
- Is evacuation or invacuation necessary and safe?

**Access routes**
- Update with routes that are safe to use
- Clarify routes which are blocked
- Nominate and search the RVP

**Number of casualties**
- List type and severity
- Approximate number of dead, injured, survivors and witnesses

**Emergency services**
- List those services present and those required
- Conduct a joint dynamic hazard assessment with the emergency services

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Cyber security

## 10 STEPS TO CYBER SECURITY

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber-attacks.

| | | |
|---|---|---|
| 1 | **Set up your Risk Management Regime** | Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers. |
| 2 | **Network Security** | Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls. |
| 3 | **User education and awareness** | Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks. |
| 4 | **Malware prevention** | Produce relevant policies and establish anti-malware defences across your organisation. |
| 5 | **Removable media controls** | Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system. |
| 6 | **Secure configuration** | Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices. |
| 7 | **Managing user privileges** | Establish effective management processes and limit the num ber of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs. |
| 8 | **Incident management** | Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement. |
| 9 | **Monitoring** | Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack. |
| 10 | **Home and mobile working** | Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest. |

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Search planning

| | Yes | No | Unsure |
|---|---|---|---|
| Do you train, rehearse and update your search plan regularly? | ☐ | ☐ | ☐ |
| Do you maintain your search regime for the lifecycle of the event including prior to the commencement, during and post-event? | ☐ | ☐ | ☐ |
| Do you carry out a zonal systematic and thorough search of your premises as a part of routine housekeeping and in response to specific incidents? | ☐ | ☐ | ☐ |
| 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 stairwells, toilets, lifts, restricted areas, car parks and service areas? | ☐ | ☐ | ☐ |
| Do concessions, sub-contractors and other service providers operating within the institution have their own search procedure and notification process when complete? | ☐ | ☐ | ☐ |
| Do you search your evacuation routes and evacuation assembly points before they are utilised? | ☐ | ☐ | ☐ |
| Are your search trained staff briefed on the grounds for search and clear what they are searching for? | ☐ | ☐ | ☐ |
| Are staff trained to deal effectively with suspicious items? | ☐ | ☐ | ☐ |
| Do you conduct unpredictable overt searches of vehicles as a visual deterrent? | ☐ | ☐ | ☐ |
| Do you have a policy to refuse entry to any vehicle/person who refuse a search request? | ☐ | ☐ | ☐ |
| Do you have sufficient staff to search effectively? | ☐ | ☐ | ☐ |
| Have you sufficient space available for the screening measures? | ☐ | ☐ | ☐ |

© NaCTSO Crown copyright 2017

| | | | |
|---|---|---|---|
| Do you have a person and vehicle, search and screening policy and plan that you can implement should there be 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 delivering crime prevention and counter terrorism messages? | ☐ | ☐ | ☐ |
| Do you have plans to search your site to deal effectively with either bomb threats or for secreted threat items? Are your staff familiar with those plans? | ☐ | ☐ | ☐ |

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Crisis response kits

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.

Your kit should include:

## DOCUMENTS

| | Yes |
|---|---|
| Instruction card/Instruction sheet (laminated), outlining roles and responsibilities | ☐ |
| 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. Activate the emergency notification system when an emergency situation occurs. | ☐ |
| Lists of customer and supplier details | ☐ |
| Contact details for emergency glaziers and building contractors | ☐ |
| Contact details for utility companies | ☐ |
| Floor plans, 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

| | |
|---|---|
| First aid kit | ☐ |
| Radios, walkie talkie communications, spare batteries and chargers | ☐ |

© NaCTSO Crown copyright 2017

| | Yes |
|---|---|
| High viz jackets and megaphone | ☐ |
| Computer back-up tapes / disks / USB memory sticks or flash drives | ☐ |
| Spare keys/security codes | ☐ |
| Torch and spare batteries / chargers | ☐ |
| Hazard and cordon tape | ☐ |
| Message pads / flip chart | ☐ |
| Marker pens | ☐ |
| General stationary | ☐ |
| Mobile telephone with credit available, plus charger Mobile Phone Charger/Portable Powerbank and adapter | ☐ |
| Dust masks | ☐ |
| Safety glasses | ☐ |
| Hard hats | ☐ |
| Camera | ☐ |
| Notebook and pen dictaphone/voice recorder | ☐ |
| Cash (for journeys home, etc.) | ☐ |

© NaCTSO Crown copyright 2017

- [ ] Space blankets/clothing
- [ ] Baby wipes
- [ ] Glucose tablets (for diabetics)
- [ ] Water

Make sure the pack is stored safely and securely off-site (in another location) or can at least be readily removed from site to an alternative location. Ensure items in the pack are checked regularly, kept up to date, and 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.

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017

# Good housekeeping

| | Yes | No | Unsure |
|---|---|---|---|
| Have you reviewed the use and location of all waste receptacles in and around your venue or event, taking into consideration their size, proximity to glazing and building support structures? | ☐ | ☐ | ☐ |
| Are the bins emptied regularly? | ☐ | ☐ | ☐ |
| Are external areas, entrances, exits, stairs, reception areas and toilets kept clean, tidy and well lit? Where possible reduce areas where items can be concealed. | ☐ | ☐ | ☐ |
| Do you keep furniture to a minimum to provide little opportunity to hide devices, including under chairs and sofas? | ☐ | ☐ | ☐ |
| Are unused offices, rooms and function suites locked? | ☐ | ☐ | ☐ |
| Do you use seals/locks to secure maintenance hatches, compacters and industrial waste bins when not required for immediate use? | ☐ | ☐ | ☐ |
| Do you screen all your mail and can you isolate your mail processing area? | ☐ | ☐ | ☐ |
| Have you tested and exercised for a terrorist incident in the last 12 months? Do staff understand their roles and responsibilities? | ☐ | ☐ | ☐ |
| Are relevant staff and deputies trained and competent in managing bomb threats? | ☐ | ☐ | ☐ |
| Do you regularly check the content of first aid kits, crisis management packs and firefighting equipment? | ☐ | ☐ | ☐ |
| Have you checked your CCTV to ensure it is working effectively and has sufficient coverage inside and outside? | ☐ | ☐ | ☐ |
| Have you taken into account the location of street vendors (e.g. flower sellers, news stands and refreshment stalls) so as not to impact upon evacuation routes, assembly points, exits or entrances? | ☐ | ☐ | ☐ |
| Are cycle racks and lockers positioned away from crowded areas? Is CCTV monitoring necessary? | ☐ | ☐ | ☐ |

Consult with security professionals, such as CTSAs, regarding the design and location of equipment such as bins, cycle and storage facilities.

© NaCTSO Crown copyright 2017

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Suspicious behaviour reporting form

**INFORM YOUR SECURITY MANAGER AND THE INCIDENT MUST BE REPORTED VIA 101 OR 999**

Date:

Time:

Location:

CCTV / other images: YES ☐ NO ☐

No of persons involved:

Activity – Why is the behaviour suspicious?
(photography, video, extended observation, accessed restricted area etc.)

**Person**

Description:

Gender

Ethnicity

Facial features

Clothes / Footware

Build

Hair style/colour

Height approx

Identifying features
(e.g. Tattoos/scars/facial hair, birthmarks, piercings etc.)

Speech/accent/wording/phases

**Equipment carried**
(Camera/bag, etc.)

© NaCTSO Crown copyright 2017

**Equipment carried**

| Seen before? | Mode of travel (on foot/tram/train/car etc) | Seen before? |
|---|---|---|
| | | |

**Vehicle Details**

| Vehicle vrm: | Make: | Model: |
|---|---|---|
| | | |

Colour:

| |
|---|
| |

| Further info: stickers/damage/body kit, etc. | Was the person challenged. (Was the person challenged. What was their response or comments) |
|---|---|
| | |

Additional information:

| |
|---|
| |

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Useful contacts

## USEFUL CONTACTS

- 999 – The emergency services
- 0800 789 321 – The confidential Anti-Terrorism Hotline
- 101 – The police non-emergency number

GO TO SECTION CONTENTS

Go to Glossary

© NaCTSO Crown copyright 2017

# Glossary

Here we explain some of the terms used in the Crowded Places Guidance.

| | |
|---|---|
| **ANPR**<br>Automatic Number Plate Recognition | |
| **ATTRO**<br>Anti-Terrorism Traffic Regulation Order | |
| **BCP**<br>Business Continuity Plan | Documented collection of procedures and information developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical functions at an acceptable predefined level. |
| **Berm** | An artificial ridge or embankment. |
| **BIM**<br>Building Information Modelling | |
| **Blast stand-off** | The distance between the explosive and the asset. |
| **BMS**<br>Building Management Systems | |
| **Bund** | An embankment. |
| **CAA**<br>Civil Aviation Authority | |
| **CAST**<br>Centre for Applied Science and Technology | Scientists and engineers who develop technological solutions to fight crime and terrorism. |
| **CBR**<br>Chemical, Biological or Radiological | |
| **CPNI**<br>Centre for the Protection of National Infrastructure | The UK government authority which provides protective security advice to businesses and organisations that provides the UK's essential services. |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **Crowded place** | Crowded Places include shopping centres, sports stadia, bars, pubs and clubs which are easily accessible to the public and attractive to terrorists.<br>NOTES:<br>(1) this definition reflects a counter terrorism perspective<br>(2) crowded places are often iconic or nodal to communities<br>(3) they face a variety of threats and risks and these must be considered in critical incident and business continuity plans<br>(4) based on intelligence, credible threat or terrorist methodology, may be considered potentially liable to terrorist attack by their crowd density or function. |
| **CTAA**<br>Counter Terrorism Awareness Advisor | Police staff who provide counter terrorism security awareness briefings and presentation about the effects of acts of terrorism, supporting the role of the CTSA. |
| **CTSA**<br>Counter Terrorism Security Advisor | A police officer or police staff who provide protective security advice on preventing and mitigating the effects of acts of terrorism. |
| **DfT**<br>Department for Transport | |
| **Directional evacuation** | Evacuation in specified directions away from threat or incident either in a pre-planned operation or having been selected as a spontaneous response following an incident.<br>NOTES:<br>(1) an element of pre-planning and rehearsal exercising is required.<br>(2) safe specified routes should have been identified prior to implementation and should be included in any plans or event documentation) |
| **Dispersal (Crowded places)** | The controlled or uncontrolled movement of people away from a threat, incident, area or event.<br>NOTES:<br>(1) this may be following an evacuation, as it is the final stage when people leave the area |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **Dynamic lockdown** | A time critical implementation of 'lockdown' used as a fast-moving tactic as a proactive option to secure areas and occupants in the best way practicable, when a spontaneous attack or incident occurs.<br>NOTES:<br>(1) this can be an effective method of protecting as many people as reasonably possible<br>(2) it must be recognised that during such a process, there are dangers of being faced with a moral decision of who might be denied entry simply due to time<br>(3) as such this must be viewed as a tactic which must be planned, practiced and trained for, but which must be based on individual time critical decisions. |
| **Egress** | Normal exiting routes at or between pre-agreed times. Usually following the termination of the event or activity. |
| **Emergency plan** | A document or collection of documents that sets out the overall framework for the initiation, management, co-ordination and control of personnel and assets to reduce, control or mitigate the effects of an emergency. |
| **EPO**<br>Emergency Planning Officer | |
| **Evacuee** | Person removed from a place of actual or potential danger to a place of relative safety. |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **Evacuation** | Removal, from a place of actual or potential danger to a place of relative safety, of people and (where appropriate) other living creatures<br>NOTES:<br>(1) this is one of several tactical options available to those tasked with the safety of crowded places<br>(2) if the evacuation is to a holding area it should be of sufficient in size to accommodate the numbers expected to be moved<br>(3) consider the need for onward movement beyond this point<br>(4) it may take place at any phase of an event or normal operating period, prior to the planned termination of activity<br>(5) it can also result in a transfer of persons to a 'safer' location from where welfare/ aid matters can be dealt with or evacuees might be vetted, to act as responders prior to dispersal<br>(6) crowd density and behaviour is complex and must be assessed by a competent person. |
| **Evacuation assembly point** | Building or area on the periphery of an area affected by an emergency, to which evacuees are directed to await transfer to a survivor reception centre or rest centre. |
| **FCO**<br>Foreign and Commonwealth Office | |
| **FPV**<br>First Person View | Where a video camera and transmitter are mounted on to a UAS and it is flown by means of video down-link, commonly displayed on video goggles or portable screen. The pilot sees from the aircrafts perspective and does not need to have sight of the model. |
| **HGV**<br>Heavy Goods Vehicle | |
| **HME**<br>Home Made Explosive | |
| **Hostile Reconnaissance** | The information gathering phase by those individuals or groups with malicious intent, it is a vital component of the terrorist attack planning process. |
| **HVAC**<br>Heating, Ventilation and Air Conditioning | UK legislation that makes it illegal to discriminate against an individual with a disability with regard to employment, education, transport, provision of goods, and facilities, premises and services. |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **HVM**<br>Hostile Vehicle Mitigation | |
| **IED**<br>Improvised Explosive Device | |
| **Invacuation** | The planned movement of people, away from a real or perceived danger, which has manifested itself outside the building or environment where people are guided to a chosen possibly central, relatively safe location.<br>NOTES:<br>(1)the holding area being sufficient in size to accommodate the numbers expected to be moved.<br>(2)consider the need for onward movement beyond this point<br>(3)it may take place at any phase of an event or normal operating period, prior to the planned termination of activity<br>(4) there is an inference within this tactical option, that a decision to initiate this process has been taken by one charged with the safety of persons, within crowded places<br>(5) crowd density and behaviour is complex and must be assessed by a competent person. |
| **Insider** | Someone who knowingly or unknowingly misuse legitimate access to commit a malicious act or damage their employer |
| **IP**<br>Internet Protocol | |
| **ISO**<br>International Organisation for Standardisation | International Organisation for Standardisation<br>ISO 22301:12 Business continuity management systems requirements. Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.<br>ISO 31000:17 Risk Management<br>ISO 310100:17 Risk assessment techniques |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **Lockdown** | Procedures to secure the external perimeter of a building, venue, event or zones within that area, in response to a known or planned threat, information or intelligence from a trusted source.<br><br>NOTES:<br>(1) this is a tactical option for those charged with controlling premises, or environments, PRIOR to them being occupied against the wishes of the site manager and is implemented to minimise harm or risk from incidents such as pre-planned protest, firearms and weapons attack or emerging risk which allows time to effectively implement it.<br>(2) crowd density and behaviour is complex and must be assessed by a competent person<br>(3) this can be an effective method of protecting as many people as reasonably possible<br>(4) it must be recognised that during such a process, there are dangers of being faced with a moral decision of who might be denied entry simply due to time<br>(5) this must be viewed as a tactic which must be planned, practiced and trained for, but which must be based on individual time critical decisions. |
| **MTFA**<br>Marauding Terrorism Firearms Attack | |
| **NCSC**<br>National Cyber Security Centre | |
| **NDFU**<br>National Document Fraud Unit | |
| **NPCC**<br>National Police Chiefs Council | |
| **NTE**<br>Night-time Economy | |
| **OR**<br>Operational Requirement | Helps organisations make smarter investments in security measures, enabling them to implement measures which are proportionate to the risks they face. |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **OSN**<br>Online Social Networking | |
| **PAS**<br>Publically Available Specification | PAS 97: 2015 Mail screening and security. A specification aimed at assisting organisations in assessing the risks they face from postal threats, and implementing appropriate screening and security measures<br>PAS 127:2014 Checkpoint security screening of people and their belongings<br>PAS 1192-5: 2015 a specification for security minded building information modelling, digital built environments and smart asset management |
| **PBIED**<br>Person Borne IED | |
| **Phased Evacuation** | An evacuation method that proceeds over several phases, often dynamically with staff proceeding to predetermine emergency points prior to the wide occupants being informed to aid most effective movement of people<br>NOTES:<br>(1) If the evacuation is to a holding area it should be of sufficient in size to accommodate the numbers expected to be moved.<br>(2) consider the need for onward movement beyond this point.<br>(3) the decision must be made by a competent operator and will have been planned for and rehearsed prior to any live implementation. It should form part of the venues emergency response plans<br>(4) crowd density and behaviour is complex and must be assessed by a competent person possible<br>(3) this must be viewed as a tactic which must be planned, practiced and trained for, but which must be based on individual time critical decisions. |
| **PMR**<br>Personal Mobile Radio | |
| **POLSA**<br>Police Search Advisor | |
| **Protected spaces** | A space internal to a building that has properties that reduce the risk to its occupants and where they can remain for a period of time, that has previously been identified and assessed” |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **PSA**<br>Pedestrian Screening Area | A remote location where pedestrians are searched prior to entry to the venue and access or ticketing is confirmed. |
| **PSV**<br>Public Service Vehicle | |
| **RCIED**<br>Radio Controlled IED | |
| **RSES**<br>Register of Security Engineers and Specialists | |
| **SECCO**<br>Police Security Coordinator | |
| **Self-evacuation** | A spontaneous, self-initiated reaction to either information or stimulus which, alarms occupants or visitors to a point where they take the decision to leave an area, en-masse in response to a real or perceived threat."<br>NOTE:<br>(1) This is often impractical to control and at times predict. |
| **SIA**<br>Security Industry Authority | |
| **SMS**<br>Security Management System | |
| **SSP**<br>Strategic Security Plan | |
| **UAS**<br>Unmanned Aircraft System | Sometimes known as drones or Unmanned Aerial Vehicles (UAVs) these vehicles do not have a pilot on-board but can be controlled with a remote control or by an on-board computer. |
| **UK Government Response Levels** | Provide a general indication of the protective security measures that should be applied at any particular time |
| **UVIED**<br>Under Vehicle IED | |

© NaCTSO Crown copyright 2017

| | |
|---|---|
| **VACP**<br>Vehicle Access Control Point | |
| **VAW**<br>Vehicle As a Weapon | |
| **VBIED**<br>Vehicle-borne IED | Commonly known as a vehicle-bomb VBIEDs are explosives placed inside a vehicle, unlike UVIED which are placed underneath vehicles. |
| **VOIED**<br>Victim Operated IED | |
| **VSA**<br>Vehicle Screening Area | A remote location where vehicles are searched prior to entry to the venue location. |
| **VSB**<br>Vehicle Security Barrier | |
| **White powders** | The phrase 'white powders' is often used in the context of mail and encompasses CBR material as well as benign materials (however, some materials may not be white and may not be powders). |
| **Zonal evacuation** | An evacuation which proceeds by emptying occupants of a specified section of a building or area, designed to either contain or remove a threat, or create a sterile working area, thereby minimising disruption to the wider environment."<br>NOTES:<br>(1) this will be a tactical option, decided upon by those charged with the safety of crowded environments<br>(2) if the evacuation is to a holding area it should be of sufficient in size to accommodate the numbers expected to be moved.<br>(3) consider the need for onward movement beyond this point.<br>(4) the decision must be made by a competent operator and will have been planned for and rehearsed prior to any live implementation. It should form part of the venues emergency response plans<br>(5) crowd density and behaviour is complex and must be assessed by a competent person. |

© NaCTSO Crown copyright 2017

See also Government Lexicon: Provides a common understanding of specific terms and phrases, meaning multi-agency working to prevent the potential serious risk of misunderstanding.

Go to the Government Lexicon website

GO TO SECTION CONTENTS

© NaCTSO Crown copyright 2017

# How to use this guide

## DOCUMENT NAVIGATION INSTRUCTIONS

**The Crowded Places Guidance is an interactive PDF**

1. When you open the PDF enable all features and click on the icon relating to your crowded place sector, this will take you to a short introduction.
2. Scroll down to the content page and click on the section you would like to read.
3. The 'Home' key will take you back to the start of the crowded place document if required.
4. Within each section you will see links to other relevant information within the guidance. Click on the link if required and follow option 7 to return to the previous page if required.
5. Built into the guidance are a number of web links that will provide you further information on that topic. Click on the web link if required, these will open in a separate window. These can be closed when you have finished with them.
6. **At the end of each chapter is a link back to the content page. Use this link to navigate around the guidance.**

**Additional functionality**

7. To return to the last page viewed, hold down the 'Alt' key and hit the 'left arrow' key simultaneously (Alt + L arrow).
8. Ctrl and L allows you to view in presentation mode so that it can take up your whole screen.
9. Ctrl and + zooms in.
10. Ctrl and- zooms out.
11. To copy a single page click 'Edit', 'Take a Snapshop', highlight the relevant area and paste into an email or document. This is a useful function if you complete the checklists.

## DISCLAIMER

This guidance is issued by the National Counter Terrorism Security Office NACTSO with the aim of helping organisations that provide protective security to Crowded Places to improve their protective security. It is general guidance only and needs to be adapted for use in specific situations. To the fullest extent permitted by law, NACTSO accept no liability whatsoever for any expense, liability, loss or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. You should make your own judgement as regards use of the guidance and seek independent advice as appropriate.

**GO TO SECTION CONTENTS**

Go to Glossary

© NaCTSO Crown copyright 2017