Counter Terrorism Protective Security Advice

for General Aviation - Revised 2014

ASSOCIATION OF CHIEF POLICE OFFICERS

POLICE SCOTLAND

produced by

NaCTSO

National Counter Terrorism Security Office

contents

This guide provides protective security advice to those who own, operate, manage or work within the General Aviation sector. 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.

This publication was withdrawn on 4 August 2020.

Part A

two general aviation

The 'General 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. It also contains crime prevention material and guidance on business continuity. **This advice is not mandatory** but may assist those engaged within the sector to enhance security to an appropriate level at their site.

If you employ staff at your site, you need to be aware of your statutory obligations under Health & Safety and Human Rights legislation. This advice may assist you in meeting appropriate standards. In the event of an incident, your written risk assessments and plans may come under scrutiny. You have a 'duty of care' to ensure the reasonable safety of everyone who works at or visits your aviation site and the buildings and training facilities therein.

To this end, in order to make the guide as appropriate as possible to your needs, it has been divided into two main parts with checklist appendices at the back.

Part A – The guidance contained within this section is for all engaged within General Aviation. From single operators to the owners of larger aerodromes, there is protective security advice that is applicable to all sites.

Part B - The second part of the guide is intended for operators or owners of aerodromes or small airports that are not governed by the National Aviation Security Programme. It gives security advice for these larger sites where any number of aviation activities take place on a regular basis and additionally, provides guidance on continuity issues.

Aviation is one of the most important and rapidly expanding industries within the United Kingdom. It is an essential element of the transport sector and as such forms part of the Critical National Infrastructure providing substantial financial input to the Gross Domestic Product.

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.

The threat from terrorism has become extremely unpredictable in terms of target and methodology. We have witnessed attacks designed to cause maximum casualties and where possible, also undermine the global economy. To that end, those involved within the industry must be more prepared than ever before.

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

The thwarted attack using liquid bombs on transatlantic airlines in 2006 and the printer toner cartridge containing explosives transported on a cargo plane in 2010 demonstrate that the threat from terrorism is real and serious. Although actual attacks in the UK have so far been infrequent, it is possible that you may come across suspicious activity or be caught in a terrorist incident. This includes a spectrum of activity that we will discuss in this book.

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

It is worth remembering that measures you may consider for countering terrorism will also work against other threats, such as theft or criminal damage. Wherever possible, any new measures should integrate with existing security arrangements.

General aviation requires all stakeholders and relevant government agencies to unite in helping prevent acts of terrorism and to maintain security of the United Kingdoms borders.

The National Counter Terrorism Security Office; in conjunction with all relevant partners, has produced this security advice for the sector.

Our Intention

Our intention is to provide advice to the following area:

The provision of protective security advice in relation to aircraft not regulated by the National Aviation Security Programme (NASP) and where applicable the aerodromes from which they operate.

The security of individual aircraft within the confines of an aerodrome remain the responsibility of the owner and aerodrome operations manager. All aircraft should be kept locked and immobilised whilst not being attended to prevent theft, tampering or other misuse.

An aerodrome is defined as:

'Aerodrome means a defined area of land intended to be used, either wholly or in part, for the arrival, departure and movement of aircraft.'

Airsites are intended to include all other locations where aircraft land or depart, for example: private air strips.

Primacy for security regulation of Aircraft and Aerodromes is the responsibility of the Civil Aviation Authority.

three managing the risk

Managing the risk of terrorism is one area of responsibility that needs to be addressed. If measures taken are sufficiently robust to your circumstances, then contingency plans drawn up to respond to an incident can be tailored appropriately and be more likely to be effective.

The General Aviation sector currently has no direct regulation. Therefore with regard to protective security, the best way to manage the hazards and risks to your site is to start by identifying the threats and vulnerabilities to your particular operation.

This will help you to decide:

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

For many General Aviation sites, simple good practice - coupled with vigilance and well practiced contingency arrangements - may be all that is needed.

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

Formulating such a risk assessment can be achieved by reading this chapter and using the checklists at the back of this guide.

Risk Management Cycle

The following diagram illustrates a typical risk management cycle:

Step One: Identify the threats

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

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

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

Your priorities for protection should fall under the following categories:

- **People** (staff, including aircrew, passengers, contractors, visitors)
- **Physical assets** (the fabric of your aerodrome, buildings, airfield etc.)
- **Information** (electronic and non-electronic data)
- **Processes** (supply chains, procedures).

You should already know what is important to your business. Tangible infrastructure such as the aircraft apron, communications and data suite, the supply of aviation fuel and aircraft spares, are integral to the operation.

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

- You should already have contingency plans to deal with any incident likely to prejudice aircrew safety or the safety of others training or using the airfield.
- You should have procedures for assessing the reliability and integrity of those you wish to employ
- You may have taken steps to protect your IT systems from viruses and hackers; these systems should be continuously updated
- You should have measures in place to limit individuals' access to parts of the airfield and incorporate appropriate access control measures. If you have reason to believe that you are at greater risk of attack because of the nature of your operation or the location of

your premises, consider what others could find out about your vulnerabilities, such as:

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

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

[See hostile reconnaissance chapter 7]

Step Three: Identify measures to reduce risk

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

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

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

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

This means that you may already have a good security regime on which you can build. Before you invest in additional security measures, review what is already in place, including staff already employed.

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

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

Due to the diversity of General Aviation, mitigating measures will vary from site to site. You should conduct regular reviews and exercises of your plans to ensure that they remain accurate, workable and up to date. You should be aware of the need to modify them to take into account any changes in your infrastructure or operation. (e.g. new building work, changes to personnel or flight operations.)

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

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

Successful security measures require:

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

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

four physical security

Physical security is important in protecting against a range of threats and vulnerabilities, including terrorism. Put in place security measures to remove or reduce your vulnerabilities to as low as reasonably practicable, bearing in mind the need to consider safety and emergency response as a priority at all times.

Your risk assessment will determine which measures you should adopt, but they can range from basic good housekeeping, such as keeping communal areas in buildings clean and tidy, to sophisticated electronic monitoring systems.

Electronic equipment must be kept maintained and be fit for the purpose it was designed for. CCTV, intruder alarms, computer security and lighting are of little benefit if they are in disrepair or not part of an integrated regime.

Action you should consider

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

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

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

Security awareness

The vigilance of all aerodrome users and staff is essential to your protective measures. They will know their own work areas or offices very well and should be encouraged to be alert to unusual behaviour or items out of place.

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

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

[See hostile reconnaissance – chapter 7]

Access control

An efficient entry system benefits the smooth flow of traffic into an aerodrome. Consideration should be given to how access could be controlled at the entrance, should the searching or screening of vehicles be required in response to a specific threat. Larger sites will 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. Consideration should be given to investing in good quality access control systems, such as magnetic swipe identification cards or proximity readers.

Security passes

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

Screening

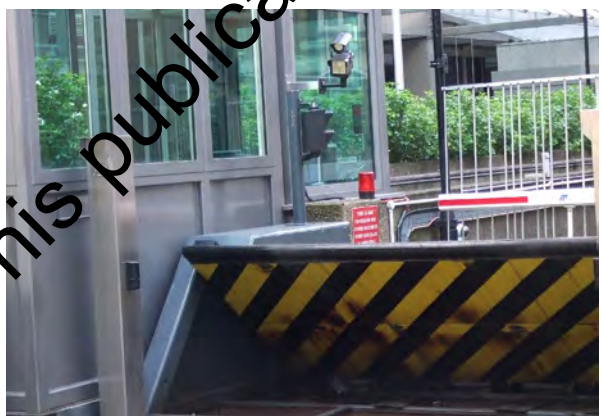
The operation of screening involves the use of electronic measures to examine people, vehicles or bags. If x-ray screening equipment is used on site, it must be carried out by trained staff. In conjunction with screening, routine searching and patrolling of premises represents another level of security; covering both internal and external areas. If you have a security force or guarding company they should keep patrols regular, though not too predictable.

[See Search Planning – Chapter 13]

Traffic Management - Vehicle Bollards & Barriers

The implementation of traffic management controls and mitigating measures are not mandatory within the General Aviation sector.

If you believe your aerodrome may be at risk from a vehicle borne improvised explosive device [VBIED] commonly known as a vehicle bomb, the basic principle is to keep all vehicles at a safe distance. Those requiring essential access should be identified in advance and checked before being allowed through. If possible, you should ensure that you have proper access control, careful landscaping, traffic calming measures and robust, well-lit barriers or bollards. Ideally, keep non-essential vehicles as far away from your building as possible.



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

Perimeter Fencing

Perimeter fencing 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. Your CTSA will be able to advise you.

Doors and windows

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

All accessible windows should have good quality key operated locks.

Many injuries 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 police CTSA.

Integrated security systems

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

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

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

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.

CCTV can be useful within non public areas of the aerodrome such as baggage make-up areas and for the aircraft stands.

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

[See CCTV – Chapter 11]

five good housekeeping

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

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

- Reduce the number of litter bins and ensure they are regularly emptied or checked
- Use clear bags for waste disposal as they provide an easier opportunity for staff to conduct an initial examination for a suspect package
- Review the use and security of any compactors, wheelie bins and metal bins to store rubbish within the aerodrome next to structures or near the apron. Do not place any bins next to or near any glazing
- Keep any public or communal areas – exits, entrances, reception areas, stairs, halls, toilets – clean and tidy
- Keep the furniture in such areas to a minimum – ensuring that there is little opportunity to hide devices
- Lock unoccupied offices, rooms and store cupboards
- Ensure that everything has a place and that things are returned to that place
- Put plastic seals on maintenance hatches
- Keep external areas as clean and tidy as possible
- Prune all vegetation and trees, especially around entrances and the perimeter fence to assist in surveillance, prevent intrusion and concealment of any packages.

[see Good Practice checklist – Housekeeping in Appendix 'A']

six chemical, biological and radiological (CBR) attacks

Since the early 1990s, concern that terrorists might use CBR materials as weapons has increased. This chapter is aimed at enhancing awareness of what is a complex subject, but should not be taken as an indication that General Aviation is at specific or significant risk of attack. However, those involved in agriculture should be aware of the potential attractiveness of both aircraft and agricultural chemicals together in the same place.

Chemical Agents: including chemical warfare agents, plus toxic agricultural, household or industrial chemicals.

Biological Agents: including bacteria or viruses that cause disease, for example anthrax, and biological toxins such as ricin.

Radiological Agents: including radiological materials used in hospitals and industry. A radiological dispersal device (RDD), often referred to as a 'dirty bomb', is typically a device where radioactive materials are combined with conventional explosives or an improvised explosive device.

Examples of recent attacks, not necessarily terrorist using CBR material:

- 1995 – Sarin gas attack [Chemical] Tokyo subway – 12 dead, 5,000 injured.
- 2001 – Anthrax letters [Biological] in the USA – 5 dead.
- 2007 – Poisoning of Litvinenko with Polonium 210 [Radiological] in London.

CBR weapons have been little used so far, and where terrorists have tried to carry out CBR attacks, they have generally used relatively simple materials. However, certain groups have expressed a serious interest in using CBR materials. Whilst the likelihood of a CBR attack remains low, vigilance within the General Aviation sector is critical, as the delivery method of airborne biological or chemical agents could be enhanced by use of light aircraft. Any suspicious activity sighted at your aerodrome should be reported immediately to police.

What you can do

- Review the physical security of aircraft, especially crop sprayers and similar types.
- Review the physical security of any toxic materials that are held on the aerodrome, and ensure proper accounting for such materials.

A basic awareness of CBR threat and hazards, combined with general protective security measures (e.g. screening visitors, CCTV monitoring of perimeter and entrance areas, being alert to suspicious letters and packages) should offer a good level of resilience. In the first instance, seek advice from your local police force CTSA.

seven hostile reconnaissance

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

- Suspicious sightings.
- Suspicious activity.

at or near:

- Crowded places.

or prominent or vulnerable:

- Buildings.
- Structures.
- Transport infrastructure.

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

Primary Role of Reconnaissance

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

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

Reconnaissance operatives may visit potential targets a number of times prior to the attack.

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

What to look for

- Significant interest being taken in the perimeter of the aerodrome including the fence line, flight paths, access and egress routes.
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas.
- People taking pictures – filming – making notes – sketching of the security measures at the access points
- Video cameras, possession of photographs, maps, blueprints etc, of critical infrastructure, including nearby electricity transformers, gas pipelines, telephone cables etc. that may serve the site.
- Possession of global positioning systems (GPS)
- Vehicles parked at the perimeter or outside buildings at the aerodrome with one or more people remaining in the vehicle, for longer than would be considered usual.
- Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation.

- Prolonged static surveillance or simple observation such as staring or quickly looking away.
- Activity inconsistent with the nature of the building.
- Vehicles, packages, luggage left unattended.
- Vehicles appearing overweight.
- Persons appearing to count pedestrians/vehicles.
- Delivery vehicles arriving at the aerodrome at other than expected times.
- Vehicles emitting suspicious odours e.g. fuel or gas.
- Noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, [bomb threats, leaving hoax devices or packages].
- The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s).
- Unusual activity by contractor's vehicles.
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or other equipment, e.g. ropes, ladders.
- Attempts to disguise identity – motorcycle helmets, hooded tops or multiple sets of clothing to change appearance.
- Constant use of different paths, and/or access routes across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together.
- Multiple identification documents – suspicious, counterfeit, altered documents etc.
- Non co-operation with security or other aerodrome personnel.
- Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories.
- In the past reconnaissance operatives have drawn attention to themselves by asking peculiar and in depth questions of employees or others more familiar with the environment. For example, the questions could be regarding security procedures and evacuation measures.
- Sightings of suspicious activity should be passed immediately to security management for CCTV monitoring if available and the event recorded for evidential purposes.

Always contact the police if a candidate for flying lessons or attempting to hire an aircraft, raises your suspicions. Is their request unusual? What is their motive for applying? Do they wish to pay in cash? Do they only wish to undertake part of the course? Have they undertaken some training before? Is your airfield the closest to their address?

Reconnaissance operatives may also seek additional information on:

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

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

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

Aviation enthusiasts can be mistaken for someone carrying out hostile reconnaissance. Where there is doubt by aerodrome staff, the police should be informed and necessary enquiries carried out.

Any 'plane spotter' that regularly attends and is known to be bona fide, can assist aerodrome staff by pointing out any other unusual activity he or she witnesses; such as a stranger mingling with the regulars and asking questions on security regimes.

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

ANY INCIDENT THAT REQUIRES AN IMMEDIATE RESPONSE – DIAL 999.

Project Pegasus
Strengthening our borders

Project Pegasus is a joint agency initiative that delivers an enhanced vigilance capability within the aviation community, providing a hostile environment for the threat from terrorism and organised crime, such as illegal immigration and smuggling to the United Kingdom.

Through enhanced criminal and counter-terrorism awareness and the exchange of information and intelligence between border policing partners and the aviation community, airfields and their environs can continue to be a safe place to live, work and relax.

For more information contact your local police force.

eight threat levels

Information about the national threat level is available on the MI5 - Security Service, Home Office and UK Intelligence Community Websites. Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response should be made with this in mind.

There is no obligation at this time for those within the General Aviation sector to respond specifically to a change in the threat level. To do so may be expensive and disproportionate to your site. However those who own, operate, manage or work within larger aerodromes, may wish to keep themselves updated with any changes to the threat level.

Threat Level Definitions

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

Response Levels

Response levels provide a broad indication of the protective security measures that should be applied at any particular time. They are informed by the threat level but also take into account specific assessments of vulnerability and risk. Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity. There are a variety of site specific security measures that can be applied within response levels, although the same measures will not be found at every location.

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

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

CRITICAL	EXCEPTIONAL
SEVERE	HEIGHTENED
SUBSTANTIAL	
MODERATE	NORMAL
LOW	

Response Level Definitions

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

What can I do now?

- Carry out a risk and vulnerability assessment that is specific to your General Aviation site.
- Identify a range of practical protective security measures appropriate for each of the response levels. Your CTSA can assist you with this.
- Make use of the good practice checklists on the following pages to assist you in your decision making process.
    - The counter measures to be implemented at each response level are a matter for individual premises or organisations and will differ according to a range of circumstances. However it must be emphasised that the aerodrome should have counter measures that complement all users.
    - 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.

Part B

nine aerodrome security planning

Installing good protective security measures will act as an investment for your site.

The Security or Aerodrome Manager should already have responsibility for the following key areas:

- the production of a security plan based on the risk assessment
- the formulation and maintenance of a search plan
- the formulation and maintenance of other contingency plans dealing with bomb threats, suspect packages and evacuation
- liaising with the police, other emergency services and local authorities
- arranging staff training where appropriate, including his/her own deputies and conducting briefings/debriefings
- conducting regular reviews of the plans.

For independent and impartial counter terrorism advice and guidance that is site specific, the Security Manager should establish contact with the local police **Counter Terrorism Security Advisor [CTSA].** All UK Police Forces have CTSAs and they can be contacted through your nearest police station or via the force website.

Your CTSA can:

- help you assess the threat, both generally and specifically
- give advice on physical security equipment and its particular application to the methods used by terrorists. The CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation
- facilitate contact with emergency services and local authority planners to develop appropriate response and contingency plans
- identify appropriate trade bodies for the supply and installation of security equipment
- offer advice on search plans.

The CTSA is fully supported by the National Counter Terrorism Security Office [NaCTSO] and the Centre for Protection of National Infrastructure [CPNI]. This ensures a nationally consistent standard of advice to the sector.

Creating your Security Plan

The Security or Aerodrome Manager should aim to produce a plan that has been fully exercised, and which is regularly audited to ensure that it is still current and workable.

Before you invest in additional security measures, review what is already in place, including known weaknesses such as blind spots in your CCTV system.

When creating your security plan, consider the following:

- details of all the protective security measures to be implemented, covering physical, information and personnel security
- instructions on how to respond to a threat (e.g. telephone bomb threat)

- instructions on how to respond to the discovery of a suspicious item or event
- a search plan
- evacuation plans and details on securing the site and equipment to the best of your ability in the event of a full evacuation
- your business continuity plan
- a communications and media strategy should be considered

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

1. **Do not touch suspicious items**
2. **Move everyone away to a safe distance**
3. **Prevent others from approaching**
4. **Notify the police**
5. **Communicate safely to staff and airfield users**
6. **Use hand-held radios or mobile phones away from the immediate vicinity of any suspicious item, remaining out of line of sight and behind hard cover**
7. **Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.**

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

ten access control

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private side.

Risk assessment

Refer back to **'managing the risk'** and decide the level of security you require before planning your Access Control system. Take into account any special features you may require.

If your assessment suggests that such a system is required, then the following elements need to be considered;

Appearance

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

Ease of access

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

Training

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

System maintenance

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

Interaction

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

Compliance

Are you compliant with:

Equality Act 2010

The Human Rights Act 1998

The Data Protection Act 1998

Regulatory Reform (Fire Safety) Order 2005

Health and Safety at Work Act 1974

Objectives

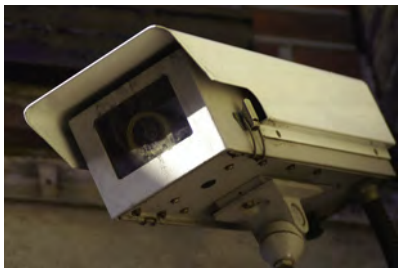
Are your security objectives being met? If necessary, carry out a further risk assessment and address any shortcomings accordingly.

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

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

See Good Practice Checklist – Access Control to Aerodrome and GA Sites in Appendix 'B'

eleven cctv guidance



If you have a Closed Circuit Television [CCTV] system, or are contemplating installing one, ask yourself the following questions:

- Does your CCTV system currently achieve what you require it to do? Do you need it to confirm alarms, detect intruders through gates or over fences and produce images of evidential quality?
- Are the CCTV cameras in use for the protective security of your aerodrome integrated with those used to monitor other activities, such as checking delivery vehicles?

The Centre for the Protection of National Infrastructure (CPNI) and the National Counter Terrorism Security Office (NaCTSO) have advice on their websites regarding the use and installation of CCTV systems as well as the 'CCTV Operational Requirements Manual' (Ref: 28/09). To view this advice visit;

- www.cpni.gov.uk
- www.nactso.gov.uk

CCTV cameras should cover the entrances and exits to your aerodrome and other areas that are critical to the safe management of any event at the site and to the security of your business. Constantly monitor the images captured by your CCTV system or regularly check recordings for suspicious activity ensuring at all times full compliance with the Data Protection Act 1998 which should be specified in your CCTV Data Protection Policy.

Consider also the following points:

- Ensure the date and time stamps of the system are accurate and synchronised
- Regularly check the quality of recordings
- Digital CCTV images should be stored in accordance with the evidential needs of the police. Refer to UK Police Requirements for Digital CCTV Systems on the NaCTSO website
- Ensure that appropriate lighting complements the system during daytime and darkness hours
- Keep any recorded images for at least 31 days
- Use good quality media and check it regularly by checking that backups are operating correctly.
- Ensure the images recorded are clear – that people and vehicles are clearly identifiable.
- Check that the images captured are of the right area
- Implement standard operating procedures, codes of practice and audit trails
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.

See Good Practice Checklist – CCTV in Appendix 'C'

twelve cargo and mail handling

Most aerodromes receive large amounts of cargo, mail and other deliveries and this offers a possible route into your sector for terrorist activity. If this is a concern, the following guidance may be applicable to your site, particularly if you have a separate cargo and mail handling building.

Suspicious Cargo and Mail

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

Suspicious packages designed to cause harm can be: explosive or incendiary (the two most likely kinds), or chemical, biological or radiological.

Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.

All cargo should be checked prior to loading on to an aircraft. Cargo or a letter containing a bomb will probably have received fairly rough handling by couriers or in the post and so is unlikely to detonate through being moved, but any attempt at opening it, however slight, may cause it to function. Unless delivered by courier, it is unlikely to contain a timing device. Bombs inside cargo or letters may come in a variety of shapes and sizes; a well-made one will look innocuous but there may be telltale signs.

Indicators to Suspicious Packages

- It is unexpected or of unusual origin or from an unfamiliar sender
- There is no return address or the address cannot be verified
- It is poorly or inaccurately addressed (eg. incorrect title, spelt wrongly, title but no name, or addressed to an individual no longer with the company
- The address has been printed unevenly or in an unusual way
- The writing is in an unfamiliar style
- There are unusual postmarks or postage paid marks
- A Jiffy bag, or similar padded envelope, has been used
- It seems unusually heavy for its size. Most letters weigh up to about 28g or 1 ounce, whereas most effective letter bombs weigh 50-100g and are 5mm or more thick
- It has more than the appropriate value of stamps for its size and weight
- It is marked 'personal' or 'confidential'
- It is oddly shaped or lopsided
- The package is heavily taped or the envelope flap is stuck down completely (a harmless letter usually has an ungummed gap of 3-5mm at the corners)
- There is a pin-sized hole in the envelope or package wrapping
- There is a smell, particularly of almonds or marzipan
- There is an additional inner package, and it is tightly taped or tied (however, in some organisations sensitive or 'restricted' material is sent in double envelopes as standard procedure).

Chemical, biological or radiological materials in cargo

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

- Unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container
- Unexpected sticky substances, sprays or vapours
- Unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres
- Strange smells, e.g. garlic, fish, fruit, mothballs, pepper, meat, rotten. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless
- Stains or dampness on the packaging
- Sudden onset of illness or irritation of skin, eyes or nose. CBR devices containing finely ground powder or liquid may be hazardous without being opened.

What you can do:

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

Planning your cargo or mail handling procedures

Although any suspect item should be taken seriously, remember that the vast majority prove to be false alarms. Some may indeed be hoaxes. Try to ensure that your procedures, while effective, are not needlessly disruptive. Take the following into account in your planning:

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

thirteen search planning

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

The following advice is generic for most sites, but recognises that the size and usage of aviation sites differ greatly around the UK.

Advice and guidance on searching is available from your local CTSA or Police Search Advisor [PoISA].

Search Plans

- Search plans should be prepared in advance and staff should be trained in them.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire site is searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to evacuate the site, or part of it, in response to a threat, you will also need to search it in order to ensure it is safe for re-occupancy. The emergency services may assist with this, however they will not be as familiar with the site as a member of staff or on site security personnel.
- The member(s) of staff nominated to carry out the search do not need to be expert in explosives or other types of device but they must be familiar with the place they are searching. They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.
- Ideally, searchers should search in pairs, to ensure searching is systematic and thorough.

Action You Should Take

Divide your aerodrome into sections. If the site is organised into separate elements such as flying school, parachute school etc. these should be identified as separate search sectors. Each sector must be of a manageable size.

The search plans should have a written checklist - signed by the aerodrome security manager following a search to show which areas have been completed.

Remember to include all offices, hangars, storage areas, stairs, corridors etc. within the search plan, as well as car parks, fuel stores, aircraft stands and other areas outside buildings.

If evacuation is considered or implemented, then a search of the evacuation point(s), the routes to them and the surrounding area should also be made.

Consider the most effective method of initiating the search. If your site has staff, you could use personal radios or pagers.

Exercise your search plan regularly. The searchers need to get a feel for the logical progression through their designated area and the length of time this will take. They also need to be able to search without unduly alarming any other persons using the site if the search is being carried out discreetly.

Searching of persons entering the Aerodrome

The security of your Aerodrome relies on having some control over persons entering it. The security levels and state of alert will differ based on threat and other factors, such as a VIP visit.

If your site has a designated 'Restricted Area' and there is no statutory search regime, it may be best for the owner of the aerodrome to instigate a policy of search as a condition of entry at specified times. This condition should be clearly displayed at the entrances to the site.

Dependent on the threat this search could be restricted to random bag searches or at times of a high security risk extend up to full body searches of every person entering the aerodrome. Security officers may only search people of the same gender.

Consider the following

- Ensure that aerodrome regulations include a right to refuse entry unless searched.
- Ensure that all staff, including temporary staff have a clause within their contracts allowing them to be searched.
- Ensure you have properly briefed those designated to conduct the searching of their powers and what they are searching for.
- Ensure the search areas have sufficient space.
- Ensure you have sufficient staff to carry out the searches.
- Experience shows that when there is a real threat from terrorism, most persons not only accept searching, they actually expect to be searched. It instils confidence in the security regime at the aerodrome.

See Good Practice Checklist - Searching in Appendix 'D'

fourteen evacuation planning

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

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

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

The biggest dilemma facing anyone responsible for an evacuation plan is whether to evacuate and how to judge where the safest place might be. The following advice will help you reach a decision. For example, if an evacuation route takes people past a suspect device outside your building, or through an area believed to be contaminated, external evacuation may not be the best course of action.

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

The decision to evacuate will normally be the responsibility of the aerodrome security manager, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation.

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

Planning and initiating evacuation should be the responsibility of the security manager and it is dependant on the size of the site and the location of the suspect item.

Plans may include:

- Full evacuation outside a building.
- Evacuation of part of a building, if the device is small and thought to be confined to one location (e.g. a letter bomb found in the post room).
- Full or partial evacuation to an internal safe area, such as a protected space, if available.
- Evacuation of all staff apart from designated searchers.

Evacuation

Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. Appoint people to act as marshals and as contacts once the assembly area is reached. Assembly areas should be a minium of 100, 200 or 400metres away dependant upon the size of the item. 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 areas for incident

evacuation as well as those for fire evacuation and that the two are not confused by those responsible for directing members of the public to either.

Car parks should not be used as assembly areas and furthermore assembly areas should always be searched before they are utilised.

Staff with disabilities should be individually briefed on their evacuation procedures.

In the case of suspected:

Letter or parcel bombs

Evacuate the room and the floor concerned along with the two floors immediately above and below.

Chemical, Biological and Radiological Incidents

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

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

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

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

Protected Spaces

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

Since glass and other fragments may kill or maim at a considerable distance from the centre of a large explosion, moving staff into protected spaces is often safer than evacuating them into the open. 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 inward.
- Away from windows, external doors and 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, because the blast can travel up them. If, however, the stair and lift cores are entirely enclosed, they could make good protected spaces.
- Avoiding ground 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 or your Counter Terrorism Security Adviser. They have knowledge of explosive effects.
- Do not neglect the provision of toilet facilities, seating, drinking water and communications.
- Consider duplicating critical systems or assets in other buildings at sufficient distance to be unaffected in an emergency that denies you access to your own. If this is impossible, try to locate vital systems in part of your building that offers similar protection to that provided by a protected space.

Communications

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

It is essential to have adequate communications within and between protected spaces. You will at some stage wish to give the all clear or tell staff to remain where they are, move to another protected space or evacuate the building.

Communications may be by public system (in which case you will need standby power), hand-held radio or other standalone systems.

Do not rely on mobile phones. You also need to communicate with the emergency services.

Whatever systems you choose should be regularly tested and available within the protected space.

Converting to open plan

If you are converting any of the buildings within the aerodrome to open-plan accommodation, remember that the removal of internal walls reduces protection against blast and fragments.

Interior rooms with reinforced concrete or masonry walls often make suitable protected spaces, as they tend to remain intact in the event of an explosion outside the building.

If corridors no longer exist then you may also lose your evacuation routes, assembly or protected spaces, while the new layout will probably affect your bomb threat contingency procedures.

When making such changes, try to ensure that there is no significant reduction in staff protection, for instance by improving glazing protection.

If your premises are already open plan and there are no suitable protected spaces, then evacuation may be your only option.

fifteen information security

The loss of confidentiality, integrity and most importantly availability of information in paper or digital format can be a critical problem for any organisation, but for an aerodrome, this can have devastating consequences.

Your confidential information may be of interest to business competitors, criminals, foreign intelligence services or terrorists. The same people may also seek to change the information your business relies on, or make the Information Technology systems unusable or unreliable.

They may attempt to attack you by breaking into your IT systems, by obtaining the data you have thrown away or by infiltrating your operation. Such attacks could disrupt your business and damage your reputation.

Before taking specific protective measures you should:

Assess the threat and your vulnerabilities

[See Managing the Risk - Chapter 3]

- To what extent is your information at risk, who might want it, how might they get it, how would its loss or theft damage you?
- Consider current good practice information security for countering electronic attack and for protecting documents.

The Centre for the Protection of National Infrastructure (CPNI) have published the 'Top Twenty Critical Security Controls' on their website www.cpni.gov.uk. This is a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.

For general advice on protecting against cyber attacks visit www.cpni.gov.uk

Cyber attacks on systems could:

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

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

The typical methods of cyber attack are:

Hacking

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

Malicious software

The techniques and effects of malicious software (e.g. viruses, worms, trojans) are as variable as they are widely known. The main ways a virus can spread are through:

- Emails.
- Interconnected systems.
- Allowing external contractors on to your network.
- Remote access (e.g. for home working).

Malicious modification of hardware

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

Denial of service [DoS]

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

Other advice

- Acquire your IT systems from reputable manufacturers and suppliers.
- Ensure that your software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites and the supplier should supply alerts by e-mail.
- Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall.
- Back up your information, preferably keeping a secure copy in another location.
- Assess the reliability of those who maintain, operate and guard your systems (refer to the section on Personnel Security on page 45).
- Consider encryption packages for material you want to protect, particularly if taken offsite - but seek expert advice first.
- Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among your staff, training them not to leave sensitive material lying around and to operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session).
- Make sure your staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords.

- Invest in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material.
- Where possible, lock down or disable disk drives, USB ports and wireless connections.
- Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.

Organisations can seek advice from the Government website -www.getsafeonline.org

Examples of cyber attacks

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

Disposal of sensitive information

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

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

The principal means of destroying sensitive waste are:

Shredding

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

Incineration

Incineration is probably the most effective way of destroying sensitive waste, including disks and other forms of magnetic and optical media, provided a suitable incinerator is used (check with your local authority). Open fires are not reliable as material is not always destroyed and legible papers can be distributed by the updraft.

Pulping

This reduces waste to a fibrous state and is effective for paper and card waste only. However, some pulping machines merely rip the paper into large pieces and turn it into a papier maché product from which it is still possible to retrieve information.

This is more of a risk than it used to be because inks used by modern laser printers and photocopiers do not run when wet.

There are alternative methods for erasing digital media, such as overwriting and degaussing.

For further information visit www.cpni.gov.uk

Before investing in waste destruction equipment you should:

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

[See good practice checklist - Information Security in Appendix 'A']

sixteen vehicle borne improvised explosive devices (VBIEDs)

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage. Whilst most general aviation sites would consider that this is an unlikely threat to their site, if you believe you may be at risk, the following guidance gives advice on this type of attack.

Once assembled, the bomb can be delivered at a time of the terrorist's choosing and with reasonable precision, depending on defences.

It can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

Building a VBIED requires a significant investment of time, resources and expertise. Because of this, terrorists will seek to obtain the maximum impact for their investment.

Terrorists generally select targets where they can cause most damage, inflict mass casualties or attract widespread media coverage. Although an attack on a general aviation site may not provide mass casualties, such an event would undoubtedly gain widespread publicity that may undermine confidence within the sector.

Effects of VBIEDs

VBIEDs can be highly destructive. It is not just the effects of a direct bomb blast that can be lethal, flying debris such as glass and metal shards can present a hazard many metres away from the seat of the explosion.

What you can do

If you think your aerodrome could be at risk from a VBIED you should:

- Ensure you have effective vehicle access controls and strict parking controls within the aerodrome.
- Insist the details of contract vehicles and the identity of the driver and any passengers approaching your goods/service areas are authorised in advance.
- Consider a vehicle search regime that is flexible and can be tailored to a change in threat or response level. It may be necessary to carry out a risk assessment for the benefit of security staff who may be involved in vehicle access control.
- Do what you can to make your buildings, particularly any terminal, blast resistant, paying particular attention to windows. Have the structures reviewed by a qualified security/structural engineer when seeking advice on protected spaces.
- Establish and rehearse bomb threat and evacuation drills. Bear in mind that, depending on where the suspected VBIED is parked and the design of your buildings, it may be safer to remain in windowless corridors or basements than outside.

[see Protected Spaces in Chapter 14]

- Consider using robust physical barriers to keep all but authorised vehicles at a safe distance. Seek the advice of your local police Counter Terrorism Security Advisor [CTSA].

[see Traffic Management Chapter 4]

- Assembly areas must take account of the proximity to the potential threat. You should bear in mind that a vehicle bomb delivered into your building or through the front of your premises could have a far greater destructive effect on the structure than an externally detonated device.
- Train and rehearse your staff in identifying suspect vehicles, and in receiving and acting upon bomb threats. Key information and telephone numbers should be prominently displayed and readily available.
- It should be emphasised that the installation of physical barriers needs to be balanced against the requirements of safety and should not be embarked upon without full consideration of planning regulations.

[See Good Practice Checklist - Access Control in Appendix 'B']

seventeen suicide attacks

The use of suicide attacks, with or without bombs, is a very effective method of delivering a terrorist act to a specific location. Suicide operatives may carry a device on their person, or utilise a vehicle, plane or vessel to deliver an attack to a target. These attacks are generally perpetrated without warning. The preferred targets being:

- Places of high crowd density
- Symbolic locations
- Key installations.

Whilst many General Aviation sites may not fall within this criteria, awareness should be brought to those within the sector, as aviation may provide a delivery method for a terrorist attack.

If you believe your site may be vulnerable to this type of attack, the following guidance may assist you identify and mitigate this risk.

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

- Using physical barriers to prevent a hostile vehicle from driving into your aerodrome through access points or across any traversable land.
- Denying access to any vehicle that arrives at your access points without prior notice and holding vehicles at access control points until you can satisfy yourself that they are genuine.
- Wherever possible, establishing your vehicle access control point at a distance from any critical infrastructure and briefing staff to look out for anyone behaving suspiciously. [Many attacks are preceded by reconnaissance or trial runs. Ensure that such incidents are reported to the police].
- Robust and covert security arrangements are known to have thwarted attacks.
- There is no definitive physical profile for a suicide operative, so remain vigilant and report anyone suspicious to the police.

[See Hostile Reconnaissance - Chapter 7]

eighteen man portable air defence systems (MANPADS)

Terrorist attacks using this methodology have been attempted in the Middle East and Africa against commercial and military aircraft. Further information on defending your site from this type of attack can be obtained from your local CTSA.

What you can do

- Report all suspicious activity within and around the aerodrome perimeter to the police. If you believe it is urgent, dial '999'.

nineteen high profile events

There may be occasions when your aerodrome, for a variety of reasons, may be subject to a high profile event.

This may be an air show or 'open day' or involve the attendance of a VIP or celebrity using the aerodrome, that results in publicity and attendant members of the press and additional crowd density.

There may be the need for an appropriate security response and increased vigilance. In certain cases the local police may appoint a police Gold Commander [Strategic Commander in Scotland] with responsibility for the event; who may in turn, appoint a Police Security Co-ordinator (SecCo) and/or a Police Search Adviser (POLSA).

Police Security Co-ordinator - SecCo

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

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

A number of options and resources are available to the SecCo, which will include liaison with the aerodrome security and operations staff, to identify all the key individuals, agencies and departments involved in the event as well as seeking advice from the relevant CTSA.

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

Police Search Adviser - PolSA

The SecCo may deem it necessary to appoint a Police Search Adviser (PolSA) to a high profile event.

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

A report, including the PolSA assessment, recommendations and subsequent search plan will be submitted through the SecCo the Gold/Strategic Commander.

twenty firearm and weapons attack

Attacks involving firearms and weapons are still infrequent but it is important to be prepared to cope with such an incident.

The important advice below will help you plan.

In the event of an attack take these four actions:

Stay Safe

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

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

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

IF YOU CAN'T ESCAPE - consider locking yourself and others in a room or cupboard.

Barricade the door then stay away from it.

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

See

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

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

Tell

Do not assume that others have already contacted Police. Therefore contact POLICE immediately by dialling 999 or via your control room, giving them the information shown under 'See'.

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

Act

Carry out the following **if safe to do so**.

- Secure your immediate environment and other vulnerable areas.
- Keep people out of public areas.
- Move away from the door and remain quiet until told otherwise by **Emergency Services** or if you need to move for safety reasons.

Armed Police

In the event of an attack involving firearms a Police Officer's priority is to protect and save lives.

Please remember:

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

Officers may be armed and may point guns at you.

They may have to treat the public firmly.

Follow their instructions; keep hands in the air/ in view.

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

Plan

Consider the following when planning for a firearms / weapons incident

1. How would you communicate with staff, public, neighbouring premises etc.
2. What key messages would you give to them in order to keep them safe?
3. Have the ability to secure key parts of the building to hinder free movement of the gunmen.
4. Does your location store NHS Medical Bags for use by paramedics to treat casualties of such an incident? Does your staff know the location of these bags?
5. Think about incorporating this into your emergency planning and briefings.
6. Test your plan.

If you require further information then please liaise with your immediate Supervisor, who can take further advice from a Counter Terrorism Security Advisor (CTSA).

twenty-one communication

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

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

It should be remembered that in the event of a terrorist attack, mobile telephone communication may be unavailable due to excessive demand. Security issues should be discussed and determined at Senior Management level and form a part of your aerodrome's culture. Security and Operations managers should meet regularly with staff to discuss security issues and encourage staff to raise their concerns about security.

All security issues should be highlighted to your Police Counter Terrorism Security Advisor.

[See Good Practice Checklist - Communication in Appendix 'I']

twenty-two personnel security

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the co-operation of an 'insider'. This could be an employee or any contract or agency staff (e.g. cleaner, caterer, aviation engineer, security guard) who has authorised access to your premises. He or she may already be working for you, or may be someone newly joined who has infiltrated your organisation in order to seek information or exploit the access that the job might provide.

What is personnel security?

Personnel security is a system of policies and procedures which seek to manage the risk of staff or contractors 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 seeks to minimise the risks.

It does this by ensuring that organisations employ reliable individuals, minimising the chances of staff becoming unreliable once they have been employed, detecting suspicious behaviour, and resolving security concerns once they have become apparent.

This chapter refers mainly to pre-employment screening, but organisations should be aware that personnel screening should continue throughout the period of employment.

Further information regarding ongoing Personnel Security can found at www.cpni.gov.uk

Understanding and assessing personnel security risks

Organisations deal regularly with many different types of risk. One of them is the possibility that staff or contractors will exploit their position within the organisation for illegitimate purposes. These risks can be reduced but can never be entirely prevented. Instead, as with many other risks, the organisation should employ a continuous process for ensuring that the risks are managed in a proportionate and cost-effective manner.

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.

Pre-employment Screening

Personnel security involves a number of screening methods, which are performed as part of the recruitment process and 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.

Pre-employment screening seeks to verify the identity and 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.

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 involving illegal activity, the police should be informed.

Pre-employment checks may be performed directly by an organisation or this process may be sub-contracted to a third party. In either case the company 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?

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.

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 roll) 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. CPNI's guidance on pre-employment screening has been updated to reflect this. More detailed information can be found at www.cpni.gov.uk

More detailed information can be found on UK Visas and Immigration website www.gov.uk

Qualifications and employment history

The verification of qualifications and employment can help identify those applicants attempting to hide negative information such as a prison sentence or dismissal. Unexplained gaps should be explored.

Qualifications

An accountant was found to be defrauding a National Infrastructure organisation. When the case was investigated it was found that the individual was not fully qualified and had lied about education qualifications during interview.

When confirming details about an individual's qualifications it is always important to:

- Consider whether the post requires a qualifications check.
- 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.

Employment checks

For legal reasons it is increasingly difficult to obtain character references, but past employers should be asked to confirm dates of employment.

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).
- Confirm details (dates, position, salary) with Human Resources departments.
- Where possible, request an employee's reference from the line manager.

Criminal convictions

A criminal conviction - spent or unspent - is not necessarily a bar to employment. The Rehabilitation of Offenders Act 1974 and the Rehabilitation of Offenders (Northern Ireland) Order 1978 establish that a criminal conviction becomes spent if an offender remains free of further convictions for a specified period. The length of the rehabilitation period depends on the sentence given, not the offence committed. The Act therefore provides the individual with protection from the unfair disclosure of criminal records data, for example to prospective employers, when there is deemed to have been a successful rehabilitation of the offence in question. A conviction is described as unspent if the rehabilitation period associated with it has not yet lapsed.

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:

1. completes a criminal record self-declaration form, or

2. applies for a Basic Disclosure certificate from Disclosure Scotland or Access NI.

The options are explained in detail in Pre-Employment Screening - 'A Good Practice Guide' on the CPNI website www.cpni.gov.uk

Financial checks

For some posts it may be justifiable to carry out financial checks, for example where the employee's position requires the handling of money. Interpreting the security implications of financial history is not straightforward and will require each organisation to decide where their thresholds lie (e.g. in terms of an acceptable level of debt).

There are a number of ways in which financial checks can be carried out. General application forms can include an element of self-declaration (for example in relation to County Court Judgements (CCJs)), or the services of third party providers can be engaged to perform credit checks.

Contractor recruitment

Aerodrome and other aviation sites employ a wide variety of contract staff. It is important to ensure that contractors have the same level of pre-employment screening as those permanent employees with equivalent levels of access to the sensitive areas of the site, be they premises, systems, aircraft or other information data.

Contracts should outline the type of checks required for each post and requirements should be cascaded to any sub-contractors. Where a contractor or screening agency is performing the checks they should be audited.

Overseas checks

As the level of outsourcing rises and greater numbers of foreign nationals are employed within the aviation infrastructure, 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 long-standing 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:

1. *Request documentation from the candidate.*
2. *Hire a professional external screening service.*
3. *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.

[See Personnel Security Checklist in Appendix 'E']

twenty-three business continuity

Business continuity

Is your General Aviation site able to cope with an incident or attack and return to normality as soon as possible?

An attack on a vulnerable point or supplier can also impact on business continuity. This is particularly important for smaller sites that may not have the resources to withstand even a few days of financial loss.

The National Counter Terrorism Security Office has produced three guidance documents; 'Expecting the Unexpected', 'Secure in the Knowledge' and 'Counting the Cost', and two training seminars; 'Project ARGUS' and 'Project Griffin', on preparing for, dealing with and recovering from a terrorist attack.

More details can be found on our website www.nactso.gov.uk

Loss of reputation

A loss of reputation for your aviation site can make all the difference for future business. The site that handles and recovers well from an attack, or is perceived to have done so, will encourage back existing users as well as generating future business.

Make sure that your site has adequate insurance to cover terrorist threats - consult your insurance company or broker.

There is limited value in safeguarding your own business premises in isolation. Take into account neighbouring buildings or facilities that may be owned by others.

All of us have a duty to prevent a terrorist event occurring. Much of the information contained within this book is designed to act as an aide - memoire that promotes security and good practice. It should be utilised alongside any requirements of the National Aviation Security Programme to supplement the security arrangements at your airport or aerodrome.

Staff and emergency services have found their effectiveness has been greatly improved by thorough preparation. Therefore, as well as reading this book, you are urged to carry out a series of contingency planning and 'Tabletop' exercises with relevant local agencies at your site. This will play an important role in quickly stabilizing and dealing with an actual event should it occur.

Part C

good practice checklists

The following checklists are intended as a guide for those who own, operate, manage or work within the General Aviation sector to assist them in identifying the hazards and risks associated with counter terrorism planning.

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

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

- Have you consulted your police CTSA, local authority and local fire and rescue service?
- Who else should be included during consultation?
- Which measures can be implemented with ease?
- Which measures will take greater planning and investment?

appendix a

Housekeeping Good Practice

	Yes	No	Unsure
Have you reviewed the use and location of all waste receptacles in and around your aerodrome and within buildings, taking into consideration their size, proximity to glazing and building support structures?			
Do you keep external areas, entrances, exits, stairs, reception areas and toilets clean and tidy?			
Do you keep furniture to a minimum to provide little opportunity to hide devices, including under chairs and sofas?			
Are unused offices, rooms and workshops 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 cargo and mail and can you isolate your cargo and mail processing area?			
Are your reception staff and deputies trained and competent in managing telephoned bomb threats?			

appendix b

Access Control to Aerodromes and General Aviation Sites

	Yes	No	Unsure
Do you prevent all vehicles from entering the site until they are authorised by your security?			
Do you have in place robust physical barriers to keep all but authorised vehicles at a safe distance and to mitigate against a hostile vehicle attack?			
Is there clear demarcation identifying the public and private areas of your aerodrome?			
Do your staff, including contractors, cleaners and other employees wear ID badges at all times when on site?			
Do you adopt a 'challenge culture' to anybody not wearing a pass airside or within restricted areas?			
Do you insist that details of contract vehicles and the identity of the driver and any passengers requiring permission to park and work within the aerodrome are authorised in advance?			
Do you require driver and vehicle details of waste collection services in advance?			
Do all business visitors to your aerodrome management and administration areas, have to report to a reception area before entry and are they required to sign in and be issued with a visitors pass?			
Are business visitors' badges designed to look different from staff badges?			
Are all business visitors' badges collected from visitors when they leave the site?			
Does a member of staff accompany business visitors at all times while in the private sections of the aerodrome?			

appendix C

CCTV

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

appendix d

Searching

	Yes	No	Unsure
Do you exercise your search plan regularly?			
Do you carry out a sectorised, systematic and thorough search of your aerodrome as a part of routine housekeeping and in response to a specific incident?			
Does your search plan have a written checklist - signed by the searching officer as complete for the information of the aerodrome operations or security manager?			
Does your search plan include toilets, any lifts, corridors, car parks and service areas?			
Have you considered a vehicle search regime that is flexible and can be tailored to a change in threat or response level?			
Do you conduct random overt searches of vehicles as a visual deterrent?			
Do concessionaires, sub-contractors and other service providers operating within the aerodrome have their own search procedure with notification to inform management when complete?			
Do you make use of your website/publications to inform contractors, visitors, of your searching policies as well as crime prevention and counter terrorism messages?			
Do you have a policy to refuse entry to any vehicle whose driver refuses a search request?			
Are your searching staff trained and properly briefed on their powers and what they are searching for?			
Are staff trained to deal effectively with unidentified packages found on the premises?			
Do you have sufficient staff to search effectively?			
Do you search your evacuation routes and assembly areas before they are utilised?			

appendix e

Personnel Security

	Yes	No	Unsure
During recruitment you should require:			
Full name			
Current address and any previous addresses in last five years			
Date of birth			
National Insurance number			
Full details of references (names, addresses and contact details)			
Full details of previous employers, including dates of employment			
Proof of relevant educational and professional qualifications			
Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals			
Do you ask British citizens for:			
Full (current) 10-year passport			
British driving licence (ideally the photo licence)			
P45			
Birth Certificate – issued within six weeks of birth			
Credit card – with three statements and proof of signature			
Bank card – with three statements and proof of signature			
Proof of residence – council tax, gas, electric, water or telephone bill			
EEA Nationals:			
Full EEA passport			
National Identity Card			
Other Nationals:			
Full Passport and			
A Home Office document confirming the individual's UK Immigration status and permission to work in UK			

appendix f

Information Security

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

appendix g

Know your customer

It is of paramount importance that any person seeking to hire an aircraft or undertake flying lessons is a bona fide customer. If you have any doubts concerning the legitimacy of any person hiring or undertaking lessons in aviation, contact the **Anti Terrorist hotline: 0800 789321**

Hiring an aircraft	Yes	No	Unsure
Has the person provided authentic documentation, such as a current private pilots licence?			
Has the person provided a flying log?			
Is the aircraft being hired for a legitimate purpose?			
Is the customer known to your site or can they be verified by another aerodrome operator?			
Are they familiar with the aircraft?			

Flying Lessons	Yes	No	Unsure
Is the candidate's motive for undertaking training genuine?			
Is your flying school the nearest to the candidates home address?			
If the answer to the following questions is yes, then consideration should be given to passing details, in confidence, to the police, Anti Terrorist hotline: 0800 789321.			
Is the candidate paying for the lessons in cash?			
Does the candidate wish to only undertake part of the course i.e. only interested in practical lessons as opposed to theory.			
Is there undue urgency in their request?			
Are they reluctant to provide contact details?			
Is there anything else that you feel raises your suspicions about the legitimacy of the candidates application?			

appendix h

Cargo Awareness Checklist

If you transport cargo or supplies for a third party, it is important that you are aware of what you are carrying aboard.

	Yes	No	Unsure
Do you check all consignments going on board your aircraft?			
If contacted by a new customer, have you taken steps to check the validity of their operation?			
Do you publicise the right to search all items going aboard?			
If an item is to remain sealed, is it from a regular and trusted customer?			
Do you complete a manifest for all items going onto and off the aircraft?			

appendix i

Communication

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

What do the results show?

- **Having completed the various 'Good Practice' checklists you need to give further attention to the questions that you have answered 'no' or 'don't know' to.**
- **If you answered 'don't know' to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed.**
- **If you answered 'no' to any question then you should seek to address that particular issue as soon as possible, in accordance with your risk assessment.**
- **Where you have answered 'yes' to a question, remember to regularly review your security needs to make sure that your security measures are fit for that purpose.**

appendix j bomb threat checklist

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

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

Actions to be taken on receipt of a bomb threat:

Switch on tape recorder/voicemail (if connected)

Tell the caller which town/district you are answering from

Record the exact wording of the threat:

_____

_____

Ask the following questions:

Where is the bomb right now? _____

When is it going to explode? _____

What does it look like? _____

What kind of bomb is it? _____

What will cause it to explode? _____

Did you place the bomb? _____

Why? _____

What is your name? _____

What is your address? _____

What is your telephone number? _____

(Record time call completed:)

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

_____

Inform the premises manager of name and telephone number of the person informed:

_____

Contact the police on 999. Time informed: _____

The following part should be completed once the caller has hung up and the premises manager has been informed.

Time and date of call: _____

Length of call: _____

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

ABOUT THE CALLER

Sex of caller: _____

Nationality: _____

Age: _____

THREAT LANGUAGE (tick)

❒ Well spoken?

❒ Irrational?

❒ Taped message?

❒ Offensive?

❒ Incoherent?

❒ Message read by threat-maker?

CALLER'S VOICE (tick)

❒ Calm?

❒ Crying?

❒ Clearing throat?

❒ Angry?

❒ Nasal?

❒ Slurred?

❒ Excited?

❒ Stutter?

❒ Disguised?

❒ Slow?

❒ Lisp?

❒ Accent? If so, what type?_____

❒ Rapid?

❒ Deep?

❒ Hoarse?

❒ Laughter?

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

BACKGROUND SOUNDS (tick)

❒ Street noises?

❒ House noises?

❒ Animal noises?

❒ Crockery?

❒ Motor?

❒ Clear?

❒ Voice?

❒ Static?

❒ PA system?

❒ Booth?

❒ Music?

❒ Factory machinery?

❒ Office machinery?

❒ Other? (specify) _____

OTHER REMARKS

_____

_____

_____

_____

Signature

_____

Date _____

Print name

_____

Part D

twenty-four NaCTSO

NaCTSO

National Counter Terrorism Security Office

The National Counter Terrorism Security Office (NaCTSO), on behalf of the Association of Chief Police Officers, Terrorism and Allied Matters (ACPO TAM), works in partnership with the Centre for the Protection of National Infrastructure (CPNI) to reduce the impact of terrorism in the United Kingdom by:

- Protecting the UK's most vulnerable and valuable sites and assets
- Enhancing the UK's resilience to terrorist attack
- Delivering protective security advice across the crowded places sectors.

NaCTSO aims to:

- Raise awareness of the terrorist threat and the measures that can be taken to reduce risks and mitigate the effects of an attack
- Co-ordinate national service delivery of protective security advice through the Counter Terrorism Security Advisor (CTSA) network and monitor its effectiveness
- Build and extend partnerships with communities, police and government stakeholders
- Contribute to the development of national and international counter terrorism policy and advice.

twenty-five CPNI

CPNI
Centre for the Protection of National Infrastructure

Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure is the Government authority that provides protective security advice to business and organisations across the national infrastructure.

Its advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer.

One of these essential elements is the transport sector, without which the UK could suffer serious consequences, including severe economic damage and grave social disruption.

twenty-six NCPP

ASSOCIATION OF CHIEF POLICE OFFICERS

National Co-ordinator Protect and Prepare

The National Co-ordinator Protect and Prepare is a senior police officer who works directly to the Association of Chief Police Officers [ACPO]

The team within this department are responsible for co-ordinating the policing and security of the United Kingdoms borders through a network of Special Branch officers and through partnership engagement with other government agencies and the industry.

'Working together to secure UK ports and borders from the threat of terrorism and crime thereby reducing harm to the UK.'

twenty-seven Civil Aviation Authority

The Civil Aviation Authority (a public corporation for The Department for Transport) aims to protect the travelling public, transport facilities and those employed in the transport industry, primarily from acts of terrorism. Its aim is to retain public confidence in transport security without imposing requirements that impact on the way they travel.

The National Aviation Security Programme (NASP) monitors the protection of airports, aircraft, air passengers and air cargo with the aim of safeguarding civil aviation operations against acts of unlawful interference.

twenty-eight further publications

Publications

Protecting Against Terrorism (3rd Edition)
This 38-page booklet gives general protective security advice aimed at businesses and other organisations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk

Personnel Security: Threats, Challenges and Measures
This booklet has been developed by the CPNI. It outlines various activities that constitute a personnel security regime. As such it provides an introductory reference for security managers and human resource managers who are developing or reviewing their approach to personnel security. The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk

Risk Assessment for Personnel Security
Personnel security assessment focuses on employees, their access to the organisation's assets, the risks they could pose to the organisation and the sufficiency of countermeasures. It is the foundation of the personnel security management process. It is also crucial in helping security and human resource managers communicate to senior managers the risk to which the organisation is exposed.

Very often, clear rationales for the use of particular personnel security measures are lacking and resources are not targeted in a proportionate way. CPNI's personnel security risk assessment guidance, which is illustrated using a fictional case study, aims to help security and human resource managers to;

- Conduct personnel security risk assessments in a way that balances pragmatism with rigour.
- Prioritise the insider risks to an organization.
- Identify appropriate countermeasures to mitigate against those risks.
- Allocate personnel security resources in a way that is cost effective and commensurate with the level of risk.

Good Practice Guide on Pre-employment Screening
CPNI's Pre-employment Screening is the latest in a series of advice products on the subject of personnel security. It provides detailed guidance on pre-employment screening measures including:

- Identity checking.
- Confirmation of the right to work in the UK.
- Verification of a candidate's historical personal data (including criminal record checks).

The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk.

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

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

Counting the Cost
This book provides guidance and information that will help small and medium sized businesses to risk assess the security and resilience needs of their business, recognise threats and hazards and understand better the role of insurance. Available to download at www.nactso.gov.uk

Project Argus
Project Argus is a National Counter Terrorism Security Office initiative, exploring ways to aid the prevention, handling and recovery from a terrorist attack. It achieves this by taking businesses through a simulated terrorist attack. The event is free of charge and further information can be obtained from your CTSA.

Project Griffin
Project Griffin aims to raise awareness of Counter Terrorism issues with members of the business community and provide an important link between the police and business. Please contact your CTSA for further information.

twenty-nine useful contacts

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

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

Civil Aviation Authority
www.caa.co.uk

Home Office
www.gov.uk

Centre for Applied Science and Technology
www.gov.uk

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

Police Scotland
www.scotland.police.uk

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

Cabinet Office - Preparing for Emergencies
www.gov.uk

Chief Fire Officers Association
www.cfoa.org.uk

Get Safe Online
www.getsafeonline.org

MI5 - The Security Service
www.mi5.gov.uk

Health and Safety Executive
www.hse.gov.uk

Information Commissioners Office
(Data Protection Act) www.ico.gov.uk

Counter Terrorism Command – Anti Terrorism Hotline: 0800 789 321

notes

Acknowledgments

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

Centre for the Protection of National Infrastructure (CPNI)
Office of National Co-ordinator Protect and Prepare
Department for Transport, Aviation Security Compliance
Civil Aviation Authority
Surrey Police S.B. Ports Office, CTSA Office, Air Support Unit

Produced by the National Counter Terrorism Security Office
NaCTSO/11. 2012 (Reviewed 2014)

Home Office

CPNI
Centre for the Protection of National Infrastructure