Department for Transport

Bus and Coach Security
Recommended Best Practice

Second edition
July 2012

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website in accordance with the W3C's Web Content Accessibility Guidelines. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
Website www.dft.gov.uk

General email enquiries FAX9643@dft.gsi.gov.uk

Cover photo acknowledgements

Images on board bus: copyright © FirstGroup plc.

Image of Leeds Bus Station concourse: copyright © Metro West Yorkshire Passenger Transport Executive.

Images reproduced with kind permission of FirstGroup plc and Metro West Yorkshire Passenger Transport Executive.

recycle Printed in Great Britain on paper containing at least 75% recycled fibre.

Contents

Section 1 – Introduction

Background

1.1 The Department for Transport (DfT) sets and enforces counter terrorism security measures on a number of transport modes including aviation, the national rail network and the London Underground. DfT does not regulate the bus and coach sector for security, but it produced security guidance for the industry following requests for advice from some bus operators in the wake of the London bombings in July 2005. We have updated that original guidance here, reflecting developments in the terrorist threat and associated security advice.

1.2 This guidance has been developed to help you devise and maintain a range of best practice security measures to prevent/deter acts of violence against buses and coaches, and protect your staff and passengers, without impacting disproportionately either on the travelling public or the industry. It covers vehicles, stations/termini and depots, and generic security issues such as personnel security and building a security culture.

1.3 This guidance should enable you to gain a good understanding of the issues to consider and provide you with a range of options that you could implement, including basic measures that together with suggested enhancements you can draw on at times of heightened concern (e.g. if there is a bomb threat, or if the country moves to a higher level of threat). More information about threat levels is on the MI5 website.[1] We suggest that you check the website regularly for changes.

1.4 The three key elements underpinning the advice throughout are:

- **Security checks;**
- **Keeping secure; and**
- **Vigilance.**

1.5 Each section explains these elements and other security related practices in more detail.

1 https://www.mi5.gov.uk/output/threat-levels.html

1.6 Other recommendations are based on the experience gained in developing and putting in place effective, proportionate, viable and sustainable security measures for other transport areas, where these are relevant, and on some good practices that various operators already have in place.

1.7 We have also produced a Bus and Coach Security DVD training aid (free on request) which complements this guidance. Details of how to obtain the DVD are given at the end of this section.

How to use this guidance

1.8 This guidance is for operators of buses and coaches and owners/managers of bus and coach stations and depots. Sections 1, 2 and 3 are generic and relevant to all, 4 to bus and coach vehicles, 5 to bus stations and termini, 6 to depots. We suggest that you draw on this guidance and the accompanying DVD to develop and implement your own security regimes, tailored to your respective operations. The Quick Reference Checklist at Annex D can help you do this.

1.9 We also recommend building these measures into your contingency planning (see Section 2).

1.10 Following this guidance will help you to strengthen security, reassure your passengers and increase public confidence in using bus and coach services and facilities generally. It can also offer positive benefits in helping to reduce the risk of crime and anti-social behaviour.

Sources of advice and further guidance

1.11 Whilst this guidance and the DVD are important sources of advice, they should not be seen as the only available reference. The Centre for the Protection of National Infrastructure (CPNI) has produced a booklet called *Protecting Against Terrorism* offering general protective security advice for businesses and other organisations.[2]

1.12 You may find it helpful to contact other operators and infrastructure owners/managers (i.e. those who own and/or manage bus/coach stations and depots) in your area to consider sharing best practice. Also, if you own or run a bus station adjoining a railway station, you could consider contacting the railway station manager to discuss mutually beneficial security measures.

1.13 Local authorities prepare emergency planning guidance as a requirement under the Civil Contingencies Act and may be able to provide assistance on some aspects, e.g. contingency planning. They can also assist if you have concerns regarding the positioning of street furniture such as litter bins or cycle racks.

2 available online at: http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf?epslanguage=en-gb

1.14 Local police forces can provide advice specific to your operation. Each force has a Crime Reduction Unit, Crime Prevention Design Advisor (CPDA) and a Counter Terrorism Security Advisor (CTSA) – all of whom are a good source of free advice and assistance, and will be able to assist you in determining suitable security measures. Additionally, CTSAs promote awareness of the terrorism threat and develop positive ongoing relationships with the local business community, partner agencies and site owners to encourage a co-ordinated approach. Contact details can be found on the National Counter Terrorism Security Office (NaCTSO) website (www.nactso.gov.uk). Additionally, we recommend referring to the NaCTSO website. which cites sources of guidance on protecting crowded places.[3]

1.15 We have discussed the updated guidance with a range of stakeholders, including the Scottish and Welsh devolved administrations, the Confederation of Passenger Transport UK (CPT), the Passenger Transport Executive Group Safety and Security Group (PTEG S&SG), the Centre for the Protection of National Infrastructure (CPNI), the police, the National Counter Terrorism Security Office (NaCTSO), FirstGroup, TfL Surface Transport and Bus Operations, and West Yorkshire Metro. The guidance will be available on the DfT website and other Government/ transport related sites, so that it is accessible to a wide range of stakeholders including operators, Passenger Transport Executives and local authorities.

DfT contact details

1.16 Should you wish to know more, have any questions about bus/coach security, or want to obtain a copy of the Bus and Coach Security DVD FREE OF CHARGE, please e-mail your enquiry to landsecurity@dft.gsi.gov.uk. You can also write to the Domestic Land Transport Security Team at :

Great Minster House
33 Horseferry Road
London SW1P 4DR

1.17 For urgent enquiries arising out of normal working hours, please contact the DfT Duty Office on 020 7944 5999, fax 020 7944 5369 or e-mail duty.officers@dft.gsi.gov.uk.

3 http://www.nactso.gov.uk/AreaOfRisks/CrowdedPlaces.aspx

Section 2 – Organisational security culture

2.1 Security measures will generally be a combination of ‘‘front-line’’ physical and procedural security measures (e.g. searching, physical barriers, patrolling) and ‘‘secondary’’ measures (e.g. emergency planning, background checks, briefing/training). A ‘‘multi-layered’’ approach to security is more robust, acknowledging that no single security measure is fool-proof or capable of mitigating every type of threat.

Key actions:

- **Pre-employment checks for job applicants (e.g. ID checks);**
- **Regular staff security briefings; and**
- **Establish or review your emergency plans and test them regularly.**

2.2 The CPNI and NaCTSO have produced guidance on building organisational security culture and on personnel security measures. This is designed to help organisations to manage the risk of staff or contractors exploiting their legitimate access to their premises, information and staff for unauthorised purposes. The text at paragraphs 2.4 to 2.7 and 2.9 below is taken from that advice:

Building and embedding a security culture

2.3 Developing a security culture within an organisation is about encouraging staff to respect common values and standards towards security whether they are inside or outside the workplace.

2.4 The awareness of security amongst staff – their vigilance when conducting everyday routines, for example – is an essential part of an organisation’s protection and staff training: regular drills and internal communications play an important part. Equally important is the manner in which a business reinforces its words through its actions.

2.5 If an organisation wants its employees to act appropriately, it must provide an environment that sets an example. For instance, if staff are required to keep paperwork securely locked away but they are not

provided with sufficient storage (or broken locks are never repaired), they may question the management's commitment to security.

2.6 A security culture is about more than facilities and procedures – it is also about creating an open, trusted environment that is focused and proactive about reducing risk for everyone's benefit.

Personnel security

2.7 Personnel security concerns the possibility of the ''insider threat''. This is the threat from individuals working somewhere within the industry and abusing their access for malicious purposes. This does not only apply to terrorism – disaffected employees can also be a concern. Good personnel security ranges from sensible pre-employment measures to on-going care. The latter is to protect against existing employees who may foster a grudge against their employer, develop terrorist sympathies, or who may have been coerced out of loyalty to a family member or friend.

2.8 Although many organisations regard personnel security as an issue resolved during the recruitment process, it is a discipline that needs to be maintained throughout a member of staff's time in employment: through appraisal procedures, communication programmes, incentive schemes and even management attitudes and relationships. It should include a formal process for managing staff leaving the business.

2.9 When consistently applied, personnel security measures not only reduce operational vulnerabilities – they can also help build a hugely beneficial security culture at every level of an organisation.

2.10 Further guidance on personnel security can be found on the CPNI and NaCTSO websites.[4]

Security training

2.11 We recommend that any staff (e.g. drivers, cleaners, security staff) whose duties or tasks include the following, be briefed regularly (and if possible be given appropriate training) to ensure that they are aware of their security responsibilities and how to respond appropriately:

- Searching or checking a bus or coach;
- Passenger luggage reconciliation;
- Searching or patrolling a station or other public area;
- Controlling access into a non-public area;
- Searching by hand or screening by x-ray or other detection equipment baggage being placed in a left luggage or lost property facility; and
- Issuing passes for access to a non-public area.

4 http://www.cpni.gov.uk/advice/Personnel-security1
http://www.nactso.gov.uk/ManagingTheRisks/PersonnelSecurity.aspx

2.12 We also suggest that training be given to those appointed as or acting in the capacity of:

- Security managers;
- Directors and other senior staff whose appointments involve executive, operational or administrative responsibility for bus/coach security; and
- Managers and supervisors who have no direct responsibility for security operations or staff, but who control operations, premises or staff.

2.13 You may wish to use the free DfT Bus and Coach Security DVD (see Section 1) as part of your front-line staff training.

Administrative staff

2.14 Telephonists, receptionists, and other staff who may receive threat warnings should be briefed before taking up their duties. The responses required from them should be incorporated into appropriate staff instructions and they should be provided with checklists to remind them of the steps to take should they receive a threat warning. Their supervisors should be similarly aware of the response required, and of the need to handle information about bomb or other threats in accordance with local police advice – see Section 3.

Training records

2.15 Where your staff are given specific training, we recommend that you maintain training records that include:

- The date that each staff member took up a security related post;
- The initial/refresher training given to each member of staff; the date or dates on which it was given; and
- The signature of each staff member to confirm that they received that training.

Contingency (emergency) Plans

2.16 If you have not already done so, you should consider establishing plans to deal with any situation affecting your business and which is likely to prejudice public safety or disrupt your ability to operate normally. You will be aware that disruptive events cover a wide range of scenarios and include terrorism, fire, adverse weather, loss of service (power, fuel etc.) and loss of staff. Make sure that these also consider possible terrorist acts. For example, what would you do if there was a bomb threat to your premises – where could you relocate to in such an event, and how would you direct passengers, staff and vehicles there?

2.17 The five golden rules of contingency planning are:

- **Think about it;**
- **Plan for it;**
- **Tell staff about it;**
- **Test it; and**
- **Keep it up to date.**

2.18 Whilst many of these actions may seem to be more relevant to larger operations, effective planning and risk assessment should look at these issues, irrespective of operator size. Your Local Authority Emergency Planning Officer can help you develop risk assessments, response and contingency plans tailored to your particular operation.

Security exercises

2.19 Exercising enables you to:

- Test existing plans, procedures and systems;
- Allow staff to practise their agreed roles in a simulated and safe environment; and
- Evaluate the exercise and make any amendments to the plans as required.

2.20 Exercises give everyone an opportunity to practise your arrangements with a wide range of people and to identify any gaps in your contingency plans, against a variety of scenarios to ensure they are sufficiently robust and that your staff are familiar with them. We suggest that, where appropriate, you involve the emergency services and local authority in rehearsals and exercises. You may also join in with exercises organised by the emergency services or other transport operators. Your Local Authority Emergency Planning Officer can help you identify the correct contacts.

Section 3 – Handling threats and incidents

Key actions:

- **Print out the threat report form (Annex A);**

  Put it in a prominent place near to publicly advertised phone lines;
- **Talk about it with staff who may receive a threat call; and**
- **Use the Marauding Active Shooter Guidance (Annex B) to brief your staff.**

Received threats

3.1 Threats may be received or discovered by bus/coach staff, station staff or anyone connected to bus or coach operations. Most threats are made by telephone, and may be received directly from the people issuing the threat or through intermediaries (e.g. the media, press agencies etc.). Other types of threat might include written messages or suspicious objects. In any case, recipients should try to obtain as much information as possible about the threat in order to help assess it and identify the person issuing it. While threats are usually hoaxes intended to cause a nuisance, they must be taken seriously and assessed properly, as a small number have been for real and have preceded a terrorist or criminal act. In the first instance, we suggest you seek advice from local police on how to handle any threats received.

3.2 We recommend that any recipient of a call or message completes the Threat Report form at Annex A (which is based on the standard police threat report form) and passes it without delay to their supervisor. The supervisor should inform the police. Recipients of a written threat should keep the message and pass it to their supervisor with precise information about its discovery. Staff who are likely to receive a threat (such as customer services and sales staff), or discover a threat (such as cleaners or station patrol staff), should be briefed on the possibility and what to do on taking up their duties. Supervisors should be similarly aware of what to do and of the need to relay information about any received threat to the police. See Section 2 – Organisational security culture.

Firearms incidents

3.3 The British Transport Police (BTP) has developed a guidance note (based on advice prepared by NaCTSO) for the rail industry to provide advice on what to do if there is a ‘‘Marauding Active Shooter’’ attack affecting the network, i.e. a firearms attack, whether by a co-ordinated group of terrorists or a lone gunman. This is not, however, a rail specific issue as it potentially concerns any crowded place where people may gather. The parts of the guidance most relevant to the bus and coach industry are offered at Annex B for you to use if you wish, as best suits the needs and circumstances of your operation. For example, you could make it available to your staff in its entirety, or use it as a basis for staff briefings.

Section 4 – Security of buses and coaches

4.1 Buses and coaches operate transport networks, with passengers embarking and alighting without hindrance, at millions of stops across the country. The following provides some simple, common-sense security measures that can help to provide deterrence and passenger reassurance.

Key actions to take:

- **Check for concealed items/lost property;**
- **Passengers present a valid ticket on boarding; and**
- **Put up posters asking passengers to report any unattended items or suspicious behaviour to staff.**

Checking buses and coaches

4.2 Drivers should visually check inside their vehicle at the start and end of a route before the next journey to ensure that nothing has been concealed or left behind. Checks should include underneath seats and any storage areas, e.g. for pushchairs, bags etc. within the bus. Coach drivers or other coach crew should ensure that luggage holds, other storage compartments, overhead luggage shelves and toilets are also included in a vehicle check. These basic visual checks should only take a few minutes to complete. Examples of existing good practice in the bus and coach industry include the issue of crib cards to drivers on security consciousness and what to do if an unattended item is found – you may wish to consider introducing something similar for your own operation.

4.3 Should drivers find an unattended item, whether as part of a security check or during the course of their duties, it is important that they know what to do. One example for doing this, used to good effect on the rail network, is to apply the ‘‘HOT’’ protocol (at Annex C). This has been designed by the BTP to assist rail staff in determining whether an item or bag found is a genuine item of lost property or if it is something more suspicious. HOT has proved effective in minimising delays caused by unattended items and by identifying those which may represent an immediate hazard.

4.4 Whilst it is a useful tool, HOT may not be suitable for all environments – particularly where there is no active security presence, CCTV, search regime etc. (see Section 5 on Security at coach/bus stations, termini and interchanges). It is important that you have discussions with local police to establish a system to enable unattended items to be reported and dealt with appropriately by your staff.

Securing of bus/coach

4.5 Drivers should ensure that doors are closed when the vehicle is left unattended (e.g. at the start and end of a journey, during a comfort break or whilst parked at termini, depots or stations). This is to protect against someone entering the vehicle and potentially leaving an item on board. Where possible, passenger doors and baggage holds should be locked and, if appropriate, windows secured.

Control of passengers boarding and leaving

Buses

4.6 At the end of a route, where a security check is carried out, passengers should not be permitted to board until it is completed. Passengers should only be allowed to board if the driver is present.

Coaches

4.7 On scheduled services where tickets are issued, coach drivers should ensure that all passengers present a valid ticket before they board. If the driver is responsible for loading the luggage, passengers should not be permitted to board, where possible, until loading has been completed. If a coach makes a stop en route, e.g. at a service station, the driver should satisfy themselves that the correct passengers are re-boarding, perhaps by asking them to re-present their tickets. These measures will help to create a sense of security.

Luggage reconciliation on coaches

4.8 Coach drivers, or any other member of coach crew, if appropriate, should be responsible for loading and unloading of all items of passenger baggage. It is recommended that you engage with your local CTSA to develop appropriate procedures that minimise the risk of someone placing an item in the baggage hold without boarding the coach, or of a disembarking passenger leaving baggage behind (See Section 1 for further details).

4.9 Reconciling passengers and their luggage is important because it:

- Acts as a deterrent to potential terrorists seeking to plant a bomb;
- Gives crew a chance to visually check baggage on loading and to identify any odd behaviour. Special attention should be paid to any luggage that appears suspicious or is handled in such a way as to raise the driver's suspicions;
- Reassures passengers that you, the operator, have appropriate security measures in place; and
- Minimises potential for baggage items to be left behind and associated delays this can cause.

It is important that your staff know what to do and who to report their concerns to should they notice someone behaving suspiciously or have concerns about any suspicious items. Some examples of potentially suspicious activity are given in Section 5.

Security awareness measures for passengers

4.10 Passengers can help act as your eyes and ears, and awareness messages are very useful in promoting vigilance and providing reassurance. You could display on your vehicle security posters to remind passengers not to leave bags unattended and on what to do if they find any unattended or suspect packages or suspicious behaviour, e.g. by reporting to a member of staff or a police officer. Where buses and coaches are fitted with electronic messaging or TV screens, these can be used too. If practical, voice announcements can be made from time to time on public address systems, where fitted.

CCTV on buses and coaches

4.11 CCTV has a useful deterrent value. If CCTV has been fitted, at least one camera should provide identifiable quality images of everyone entering the vehicle, i.e. a clear image of the face plus characteristics of clothing, items carried etc. CCTV cameras positioned for **identification** purposes (i.e. for determining who is involved in an activity) should be able to produce an image size of not less than 100% standard definition screen height and ideally run at a minimum of 6 ipspc (images per second per camera). Cameras positioned for **recognition** purposes (i.e. for determining what is happening) should be able to produce an image size of not less than 50% standard definition screen height and should record at a minimum of 2 ipspc.

4.12 The system should be able to quickly export video and stills onto a removable storage medium, such as a CD or DVD, with the time and date integral to the relevant picture. Exported images should include any software needed to view or replay the pictures or be able to be replayed on a standard computer system with no additional software.

4.13 We recommend that if possible, recordings be retained for 31 days before recording media are reused, and made available to police on request. A log should be maintained to provide an audit should recordings be required by the police or other agency.

4.14 As with any technological system, things can go wrong and it is essential that good maintenance arrangements are in place so that any faults can be repaired as quickly as possible. If current CCTV systems are to be replaced, digital systems are recommended. The Home Office has published comprehensive guidance for organisations who wish to install or upgrade CCTV systems, in its *CCTV Operational Requirements Manual 2009*,[5] which concentrates on how to best to determine your requirements and ensure that the system meets these as closely as possible. Information can also be found on the CPNI website.[6]

Disposal of vehicles

4.15 Prior to disposal or sale to third parties, all vehicles should have all internal and external livery and other markings removed, along with destination blinds and other equipment such as radio and access control systems etc. to avoid potential use by others for malicious purposes.

Security enhancements – at times of increased threat

- Increase frequency of checks on board buses and coaches;
- Tighten control on passengers boarding and luggage reconciliation on coaches;
- Increase frequency of passenger security announcements/display security posters; and
- Deploy revenue control officers/other staff to travel on network, wearing hi-vis jackets.

5 http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/28_09_CCTV_OR_Manual0425.html?view=Standard&pubID=635835

6 http://www.cpni.gov.uk/advice/Physical-security/CCTV/

Section 5 – Security at bus and coach stations, termini and interchanges

5.1 Stations, termini and interchanges can be crowded places and as such be a potential terrorist target. These simple measures can help to create the feeling of a controlled environment which will help as a deterrent and provide reassurance to customers.

Key actions:

- **Arrange for your local police Counter Terrorism Security Advisor to visit you at your site (it is FREE and will include advice on protecting your premises against terrorists and criminals);**
- **Remind passengers not to leave bags unattended and advise how to report unattended/suspect packages or suspicious behaviour to staff;**
- **Fit locks/tamper proof seals to cupboards/equipment boxes in public areas;**
- **Review the area and see what ‘‘clutter’’ you can do without; and**
- **Review your litter management arrangements.**

Areas of concealment

5.2 Many bus and coach stations were designed and built at a time when security features may not have been a prime consideration. As a result many contain voids and spaces which, if large enough, could be used by a terrorist to conceal an explosive device. In addition, any ‘‘dark corners’’, particularly those that are out of view of staff and members of the public, can be potential areas of concealment.

5.3 Whilst it may not be possible to eliminate all areas of concealment some measures can be taken to reduce them. These include:

- Location of equipment – ask yourself if you are going to create a hiding space or if you can remove an existing one. Where possible, any grit bins, vending machines or other equipment boxes should be flush to walls so that nothing can be hidden behind or around any sides; tamper evident seals can be fitted to cupboards or equipment boxes that cannot be locked;
- Boarding or sealing up voids that cannot be removed e.g. under vending machines or around equipment boxes; and
- Lighting – additional lighting can be installed to improve security and make security checks easier, particularly in any darker areas.

5.4 Those involved in designing or refurbishing facilities at bus and coach stations (i.e. designers, architects and planners, as well as bus/coach station operators) can help ''design in'' security enhancing features from the outset. Clear lines of sight aid search and evacuation procedures. Curved tops on ticket machines, advertising panels and vending machines make it difficult for these to be used to place items on. Fitting them back to back with other machines, or on legs with large gaps underneath, can also make it difficult for someone to attempt to conceal an item without it looking obvious. Similarly, if planters are to be used on a station, they should be designed so as to make it impossible to hide anything underneath (i.e. no gap, or a gap so big that anything can be visible from all sides), and planting should not be so dense that it hinders searches.

5.5 A useful reference tool when designing new major bus stations, termini, and interchanges is the DfT's *Security in the Design of Station* (SIDOS) Guide. Whilst this guidance is intended for new major rail stations and rebuilds, it contains good security design principles that are more widely applicable. Other good sources of guidance available online are *Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation,*[7] *Protecting Crowded Places: Design and Technical Issues*[8] and *Crowded places: The Planning System and Counter Terrorism*.[9]

Control of access

Non-public areas

5.6 Members of the public should not be able to gain access to non-public areas such as staff rest rooms, store rooms and cleaners cupboards. All doors in public areas leading into non-public areas should be kept locked

7 http://www.cpni.gov.uk/documents/publications/2011/2011mar01-integrated_security_v1.0.pdf

8 Available from the Home Office website at http://www.homeoffice.gov.uk/publications/counter-terrorism/crowded-places/design-tech-issues?view=Binary

9 Available from the Home Office website at http://www.homeoffice.gov.uk/publications/counter-terrorism/crowded-places/planning-and-ct?view=Binary

or controlled to prevent unauthorised access. This can help to minimise areas that need to be searched and patrolled.

5.7 Ideally, keys for doors should be kept in a secure location controlled by a responsible person and a record kept of who has the key. If access is controlled by keypad, the code should only be given to persons with a legitimate need to know. We recommend that codes are changed regularly (on a frequency to be determined locally), depending on the number and turnover rate of staff with knowledge of the code. Keypad codes should be changed from the factory setting immediately on being installed.

Vehicle access

5.8 It is important to be aware of the potential threat from Vehicle Borne Improvised Explosive Devices (VBIEDs). The movement of vehicles, other than authorised buses and coaches, at stations should be strictly controlled. Ideally, access to all other vehicles should be prevented, access but where this is unavoidable (e.g. delivery to a retail outlet, access to staff parking areas) we recommend the use of access controls. Measures that can be introduced include:

- A parking permit system for staff and, where appropriate, for vehicles of visitors and contractors;
- Monitoring retail delivery vehicles to ensure that they do not stay on a station for longer than is necessary; and
- Pre-arranged deliveries only.

5.9 It is also important that you consult local police to agree a system for reporting and dealing with any suspicious vehicles, and to liaise regarding evacuation plans.

Visitors and contractors

5.10 All visitors and contractors should be required to report to the station manager or other responsible person to notify their arrival at the station. It is good practice to require them to sign in a log book. This provides important audit information, including sign in/out times and the purpose of the visit, and can be crucial in the event of an emergency evacuation of the premises.

5.11 We recommend that you give visitors a security awareness briefing along the following lines:

- If the person is issued with a visitor pass, it should be displayed prominently at all times when they are on the premises;
- If the person has a vehicle parked on site, any work/parking permits should be displayed prominently in the windscreen;
- Be vigilant when around the premises. Should a suspicious item be found, do not touch it, but contact a member of staff as soon as possible. Similarly, if a person is seen to be acting suspiciously, contact a member of staff; and
- Ensure that all doors are properly closed/locked when you are leaving, particularly those doors that lead to non-public areas. Do not allow anyone to ''tail-gate'' into non-public areas. If you are leaving a work site, ensure that it is locked and all equipment has been securely stored.

Suspicious behaviour

5.12 Staff should have established procedures to follow for reporting any suspicious behaviour on the station to supervisors and the police. Some examples of what staff should be briefed to look out for (i.e. actions which may possibly indicate potential hostile reconnaissance/activity by criminals or terrorists) are:

- Unusual packages, bags or other items in odd places (Please refer to the HOT protocol described at Annex C);
- Carefully placed (rather than dropped) items in rubbish bins; and
- People showing unusual interest in sensitive, important or less accessible areas.

Patrolling public areas

5.13 Regular patrols by uniformed staff are a good deterrent, help to reassure passengers, and can be key to finding unattended or concealed items, or detecting suspicious behaviour. Whilst dedicated and regular security patrols are the ideal, resources may not necessarily permit this.

5.14 Security checks can be shared by a number of staff and incorporated into their duties – for example by those monitoring bus stands as part of their customer service and safety duties, by cleaners as part of their routine cleaning duties and by ticketing or sales staff in ticket halls or concourse areas. Staff are familiar with their work environment, so are well placed to spot anything out of the ordinary. Checks need not be carried out during the times a station is not accessible to the public or is not open for service, but should be carried out on opening. We recommend that you

keep records of these. They need not be overly detailed, but may provide critical information when reviewing incidents that have occurred, particularly when backed up by CCTV.

5.15 We recommend that you involve managers of other organisations (tenancies etc.) occupying premises or carrying out business at the station to ensure all parts of the station security check area are properly covered and that effective lines of communication are established.

5.16 If properly planned in advance, a security check need not be too time consuming. The key considerations for you and your staff when conducting a check of public areas are:

- **Define the area** – Staff designated to undertake a check should be sufficiently briefed and aware of what is required. Asking someone to ''check the station'' is not sufficiently detailed: a start/finish point and boundaries need to be established;
- **Plans** – The process can be simplified if laminated plans of areas to be checked are produced. The plans do not need to be particularly detailed but should highlight key features of the areas (such as toilets, emergency exits etc.) to be covered;
- **Thoroughness** – Checks need to be sufficiently thorough in order to be able to detect any concealed item. Staff should pay particular attention to areas that are not in clear public view: low roofs, emergency exits, lavatories etc. Other vulnerable areas include litter receptacles and work sites. There should not be sole reliance on visual checks – doors should be physically checked to ensure they have been properly secured. Any areas beyond doors that are found to be unlocked should be checked before they are secured. It is not considered necessary to lift drains or the covers to other utilities, unscrew access panels or search areas into which unauthorised access is not possible; and
- **Sealing** – Any locations (stores) not in regular use should be secured under lock and key. When this is not possible (for safety reasons etc.), tamper evident seals are a good option. This will eliminate the need to check inside such boxes or cupboards unless the seal is no longer intact.

5.17 In summary, security checks should concentrate on areas of public space – especially those not in clear public view as terrorists do not want their bombs or their actions to be noticed. All checks should be made regularly and if possible recorded.

5.18 Should an unattended item be found, whether as part of a security patrol or during the course of staff carrying out their duties, it is important that there are established procedures to follow. One such example is to apply the HOT protocol described at Annex C and in the DfT Bus and Coach Security DVD.

Waste management

Litter bins

5.19 Litter bins provide an easy and convenient method of concealment for a device and have been used by terrorists in the past. Certain types of receptacles, such as those made of metal, concrete or plastic, pose a greater risk as they can add to blast fragmentation, which can cause serious injury and structural damage.

5.20 The following bin design recommendations are based on rail requirements but are equally valid here. Litter bins should be of a type that would not contribute to the fragmentation if an IED were to explode inside it. A recommended design is a clear plastic sack that is unobstructed from view and suspended from a metal or plastic frame, so as to be easy to inspect visually and to remove if circumstances require. They should not have a lid, unless it is a plastic one, and hoops should be attached to concrete or brick walls, away from flammable structures, or to dug-in, stand-alone wooden posts. Consideration should be given to covering bins by CCTV so that the face of anyone placing an item in the bin would be seen.

5.21 We also recommend these ‘‘do’s and don’ts’’:

Do:

- Check and empty bins regularly;
- Place bins near staffed positions (where possible) for deterrent value as well as to ensure that they do not become over-full; and
- Keep the number of bins to the lowest practicable level and monitor usage to identify those that are not really necessary.

Don’t:

- Allow litter bins to overflow (ideally they should be emptied when no more than half full); and
- Place litter bins near control rooms, evacuation routes, sources of possible fragmentation, such as overhead glass canopies, windows, mirrors etc., fire hydrants or electrical equipment.

Bulk rubbish containers and compactors

5.22 Large bulk rubbish containers (including wheelie bins, compactors and skips) should be stored in secure non-public areas where possible. However, if they are to be stored in public areas such as in car parks or adjacent to entrances, they should be emptied and checked regularly, be capable of being locked and kept so, and covered by CCTV cameras.

Recycling facilities

5.23 Recycling facilities should not be located on or adjacent to well populated areas (e.g. station concourse), next to station building walls or next to entrances or exits. Recycling facilities are not classified as bulk rubbish

containers but, if placed within a station, should be subject to the same measures as litter receptacles.

Bicycles

5.24 There is a risk that explosive devices could be concealed in bicycles, but the following recommended measures can be taken to reduce the risk of damage and injury.

Bicycle racks

5.25 Bicycle racks should be positioned with regard to the safety of passengers, staff and facilities, preferably away from crowded parts of the station such as bus stands, waiting areas, entrances, concourses and large windows. If this is unavoidable, we suggest the racks be covered by CCTV surveillance. Derelict/abandoned bicycles should be removed once adequate notice of removal has been given.

Bicycle lockers

5.26 Bicycle lockers are increasingly being used to safeguard bicycles from theft. These bring associated risk, as an explosive device could be concealed inside a cycle locker. As with cycle racks, positioning can minimise the risk (see above for recommendations). In addition, we recommend that those using the lockers do not secure them with their own padlocks. Ideally, keys and padlocks for lockers should be controlled and issued by the facility operator, with spare keys retained securely to enable lockers to be checked by staff in the event of a security incident or alert.

5.27 Solid sided bicycle lockers may be used, although lockers with mesh sides or adequate vision ports (that provide good visibility of the interior during low light conditions) are preferable and can assist in checking.

Equipment boxes

5.28 It is recommended that all equipment boxes, such as sand and grit bins, fire extinguisher boxes, first aid equipment etc., are kept shut and secured to prevent anything being concealed inside. One of the best ways of doing this is with a tamper evident seal (e.g. plastic/wire seals, stickers) that can easily be broken in the event of an emergency. A broken seal can also highlight if a box has been tampered with.

Public toilet facilities

5.29 Terrorists have in the past used toilets for concealing explosive devices. When public toilets are checked at a station, particular attention should be paid to potential areas of concealment (such as exposed cisterns). Where old style cisterns are used, a tamper evident seal could be placed on to the cistern. If refurbishment of a public toilet facility is being considered, designs that reduce or eliminate areas of concealment are preferred. Your local CPDA can advise.

Post boxes

5.30 Any post boxes located at a station should be kept locked or otherwise securely closed (apart from any opening used for the posting of mail), except when being emptied by a person authorised to collect the mail within it. The opening should be kept as small as possible to limit the size of items posted to letter format.

5.31 You should obtain advice from your local CPDA if you intend to increase the number of post boxes at a station, particularly if you are considering installing post boxes that take items larger than normal letter/small packet size.

Tenants and cleaners

5.32 Tenants and cleaners have their part to play in overall security. We recommend that you have periodic meetings with them (and indeed with all bus/coach operators at the station) at which security issues can be discussed. Tenants and cleaners should be made aware of the importance of vigilance and given details of incident reporting procedures (who to report to, what to report etc.). Tenants should also be aware of the need to secure any stock rooms and, where appropriate, monitor and supervise any delivery vehicles. Cleaners should also ensure that they lock cleaning cupboards when not in use and do not leave any cleaning equipment unattended. The importance of adhering to the security regimes in place on the premises should be emphasised – such as the wearing of passes, signing-in procedures etc.

Security awareness measures for passengers

5.33 You should remind passengers not to leave bags unattended and to report any unattended or suspect packages or suspicious behaviour to a member of staff. Security messages can be displayed on posters and information screens, and they can be delivered by regular announcements on a public address system during the times that the station is open. Staff should be trained to deal with reports from members of the public and should reassure the person that their concern or information will be taken seriously.

CCTV

5.34 CCTV has deterrent value and can be used to cover parts of stations or facilities on stations that terrorists could exploit, such as litter bins, cycle racks/lockers and doors to non-public areas. Please refer to Section 4 for further information on appropriate standards for CCTV systems.

5.35 You may wish to consider liaising with other local organisations/ operations (e.g. rail stations, local authorities etc.) to identify whether it would be useful to have compatible systems or whether their CCTV surveillance covers any part of your operation to avoid duplication. It may be possible for you to agree the positioning of your and their systems to ensure that there are no potential gaps in coverage.

Left luggage facilities

5.36 Left luggage facilities present an obvious security risk. In particular, left luggage lockers are of concern, as there is no control of persons depositing bags or items. Where left luggage lockers are installed we recommend that they are covered by CCTV. Staff should have a means of accessing the lockers – or enabling the police to do so – to check their contents – for example, in circumstances of a bomb threat. This is also relevant to any other lockers, for example customer collection lockers, at a location.

5.37 At staffed left luggage facilities you may wish to consider only accepting bags for deposit from genuine passengers (e.g. those who can present a valid ticket as evidence of travel). We recommend that luggage or other property (other than lost property) be accepted on the condition that the owner of such luggage or property agrees that it may be searched and/or screened. A record should be kept of the left luggage searched/screened.

5.38 We recommend that screening be carried out by hand searching items of luggage and their contents, or using x-ray equipment that conforms to DfT standards, if it is available. A Standard Test Piece (available from x-ray machine manufacturers) determines whether an x-ray machine meets these standards in terms of image quality and will help to ensure that performance is maintained. Where it is used, x-ray equipment should be checked regularly to ensure that it is operating correctly and be maintained in accordance with manufacturer's recommendations. Further advice on testing of x-ray equipment is available on request from the DfT Land Transport Security team at the addresses given in Section 1.

5.39 Left luggage facility operators should encourage their staff to pay particular attention to any bags that appear to be suspicious or are handled in such a way as to raise suspicions. Where a customer refuses permission to search/screen items, staff should not accept these and should notify police immediately.

Car parks

5.40 We recommend that public car parks are monitored to ensure that vehicles near to buildings are not left longer than an authorised time. If public parking is available, e.g. near station entrances or other passenger facilities, a procedure for dealing with suspicious vehicles should be agreed with local police.

Security enhancements – at times of increased threat

- Carry out more frequent and more thorough security checks of the public areas in a station;
- Remove litter bins or check them more frequently;
- Close bicycle parking facilities within the station area or require panniers to be removed before bicycles are left;
- Introduce/increase frequency of passenger security announcements/display posters;
- All staff on duty in public areas to wear hi-vis jackets or tabards;
- Withdraw luggage or other lockers from use or increase amount of screening of left luggage; and
- Deliveries are to be by prior appointment only. Details of supplier, vehicle and driver to be checked and recorded on arrival.

Section 6 – Security of depots and maintenance facilities

6.1 Although depots and maintenance garages are not crowded places in the same way as stations are, some commonsense security measures applied to them can help ensure that an item is not concealed on board a vehicle when it is in these locations. As with stations and termini, we recommend having clear signage in place both to discourage unwanted access by vehicles and people and to facilitate proper egress in emergency situations.

Key actions:

- **Arrange for your local police Counter Terrorism Security Adviser to visit you at your site. It is FREE and will include advice on protecting your premises against terrorists and criminals.**

Security controls

6.2 All sites where buses or coaches are parked when not in service should be subject to minimum security controls. This can include:

- Physical access barriers around the site such as walls and fences;
- Access control measures at all entrances to prevent unauthorised access; and
- Measures to protect buses/coaches within the site (locking of vehicles, regular patrols, or CCTV cameras to detect and monitor any unauthorised access).

6.3 Systems for recording site patrols, monitoring and checking of visitors and vehicles should be established. Identification passes should be worn at all times.

Buses/coaches on site

6.4 Any buses or coaches within the depot should be checked to ensure nothing has been concealed or left inside before they leave the depot prior to entering service and again when they are returned to a depot at the end of service. Such vehicle checks may be done by drivers or by cleaners and a record made of the checks.

Security enhancements at times of increased threat

- Carry out more frequent and more thorough security checks of the facility;
- Require all visitors to report to the facility manager, or other responsible person, on arrival;
- Escort all unexpected visitors to the site;
- Secure buses and coaches when they are not subject to maintenance work; and
- Deliveries are to be by prior appointment only. Details of supplier, vehicle and driver to be checked and recorded on arrival.

Annex A – Threat Report Form

Threat Report Form **To be completed by/with the assistance of the information recipient** **To be forwarded immediately to the supervisor** **To be retained for 12 months**			
Please record all calls if possible: **Is this call recorded?:** YES/NO			
Message: exact words (continue on extra sheet if necessary)			
WHERE is the bomb/threat?			
Bus Coach Stop Station Terminus Other	Company	Location	Details (e.g. bus/coach number, route, destination)
Did the caller seem familiar with the location described? YES?NO Why?			
If it is a bomb WHEN will it explode?			
If moved After departure In transit If opened			
Date:	Time:	Day:	Other:
WHAT does it look like?			
WHO are you?			
Name of individual: Person's location:	Name of organisation: Other:		
WHY are you doing this?			
Caller characteristics (if applicable); please circle as appropriate			
Sex:	Male/Female		

Age:	Child	Teen	Young Adult	Middle Aged	Old	Unknown

Language spoken:				
Command of language:	Excellent	Good	Fair	Poor
Voice characteristics:	Loud Rasping	Soft Pleasant	High pitched Intoxicated	Deep Other
Speech:	Fast Slow Clear Slurred Stutter Nasal Articulate Hesitant Other:			
Accent:	E.g. Scottish Irish Welsh Liverpool London Geordie Birmingham West Country Other: Foreign (specify):			
Manner:	Calm Irrational Deliberate Laughing Concerned	Angry Coherent Emotional Obscene Other:	Rational Incoherent Righteous	
Background noise:	Transport (cars trains aircraft public announcements) Domestic (kitchen television/radio music) Workplace (office machines factory) Animals Other voices Other:			
Telephone warning: background details:				
Mobile phone	Payphone	Private phone	Internal call	External call
Where automatic caller ID available, record number shown:				
Number dialled by caller: Person usually on that number:				
Other details: e.g.	What? Where found? Where stored?	Written note	Text message	E-mails
Recipient's details (must be filled in):				
Name: Phone number: Threat received at: Time: Form passed to Supervisor (name): Signature		Position: Date:		

Annex B – Marauding Active Shooter guidance

B.1 The attacks in Mumbai in November 2008 involved a co-ordinated shooting, bombing and hostage-taking spree across the city by a group of 10 terrorists. The terrorists spread out, targeting a number of locations, including a railway terminus, hotels and cafes. We have also seen the effects a lone gunman can have in the attacks by Anders Breivik in Norway in July 2011, and in the shootings involving Derrick Bird in Cumbria and Raoul Moat in Northumbria during 2010.

B.2 This guidance is intended to complement existing guidance provided on other – more familiar – forms of terrorist attack, by addressing the scenario which emerged in the Mumbai attacks. ''Marauding Active Shooter'' also covers other types of firearms incidents where a gunman is active against multiple targets. This style of attack is potentially attractive to any crowded area, so vigilance by managers and staff everywhere is important.

B.3 We are not asking bus/coach organisations or staff to put themselves in the line of fire, indeed the opposite. The overall message to staff is to NOT PUT YOURSELF AT RISK. It explains how staff and managers can help keep themselves and passengers safe, whilst assisting the authorities in dealing with the situation as swiftly and effectively as possible.

B.4 In briefing staff, or responding to staff concerns, you may like to explain:

''This guidance is not being provided in response to any specific intelligence. But the current UK threat level is SUBSTANTIAL,[10] *meaning a terrorist attack is ''a strong possibility''. Having seen the new style of attack in Mumbai, and more recent events in the UK and Norway, it is sensible that we consider the scenario, in the same way that we do with other potential (and more familiar) terrorist threats to the transport system.*

An incident of this nature could happen anywhere, particularly if it is a crowded place. A transport system is only one of many possibilities if such an attack were to happen.

10 This is subject to change. Please check the Home Office websitehttp://www.homeoffice.gov.uk/counter-terrorism/current-threat-level/ for the current country threat level

The key message is that staying safe and not putting yourself at risk is paramount. By being aware of the sorts of issues that an attack in this form raises, it will help you know the best things to do in the unlikely event of this happening here.''

B.5 Police forces in England, Scotland, Wales and Northern Ireland have been training officers using the ''Stay Safe'' package in relation to firearms attacks and are providing the following advice to the business community utilising the principles of that package:

In the event of an attack consider these actions:

Stay safe

- **Under immediate GUN FIRE** – Take cover initially, but leave the area as soon as possible – if safe to do so, e.g. if the shooters are no longer a threat to you or others in your vicinity.
- **Nearby GUN FIRE** – Leave the area immediately, if it is possible and it is safe to do so.
- **Evacuation** – Beware of location and direction of threat and evacuate away from danger. Assist others in evacuating if it is safe to do so.
- **Leave your personal belongings behind** – Do not delay your evacuation but, if possible, take a means of communication (i.e. mobile phone) with you to facilitate the giving/receiving of further safety advice.
- **Do not congregate** or allow the public to congregate at evacuation points or usual rendezvous points. Dispersal away from the danger area is vital. However, try to maintain contact with your supervisor so they are aware of your safety and location.

COVER FROM GUN FIRE (Examples)	COVER FROM VIEW (Examples)
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 – Cover from view 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. 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

Pass as much information to the **Police** as possible. Consider using **CCTV** and other remote methods where able. **NEVER** risk your **own safety** or that of **others** to gain it.

If it is safe to do so, think about the following:

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

Tell

Do not assume that others have already contacted the police. Therefore contact **POLICE** immediately by dialling 999 or via your control room, giving them the information shown under **''See''**. Using this information the police will take the necessary action to ensure where possible trains are stopped entering the affected station.

Use all **forms of communication** available to you – to inform staff, public, neighbouring premises etc. of the danger.

Act

Carry out the following actions **if it is 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 an Active Shooter firearms incident:

1. How you would 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? Do 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 your local CTSA.

Annex C – Suspicious items – using the HOT protocol

C.1 A suspicious item is one that exhibits unusual characteristics (appearance or placement) and for which a legitimate purpose cannot readily be established.

C.2 To avoid unnecessary alarm, staff should first try to identify the owner of any unattended item. If no owner can be identified, they should then apply ‘‘HOT’’. This helps staff to decide quickly whether an unattended item is typical of lost property or whether it is suspicious. It is designed with staff and customer safety in mind as well as minimising disruption to the network and wider society.

C.3 The HOT protocol has been used in the rail environment since the early 1990s and is reviewed regularly. It is based on research undertaken by BTP that indicates unattended suspicious items are typically:

Hidden – i.e. placed where they will not be readily seen or noticed as unusual;

Obviously suspicious (e.g. by physical appearance, by placement, or because of the circumstances in which they have been discovered); and

Not **T**ypical of what you would normally expect to find in that environment.

C.4 Lost property items are typically:

Not **H**idden – often left where people congregate before moving to do something else;

Not **O**bviously suspicious – they do not usually exhibit improvised wiring, timers, putty-like substances etc.;

Typical of what you would normally expect to find in that environment – a judgement made best by staff with an intimate knowledge of the area in question.

C.5 It is difficult to define comprehensively how items might appear ''obviously suspicious'' from their appearance. However, from experience, a suspicious item may display one or more of the following features:

(a) external wiring;

(b) visible batteries;

(c) switches;

(d) timers;

(e) circuit boards;

(f) wire passing from one package to another;

(g) items secured by plastic adhesive tape;

(h) annotations (e.g., ''ON'', ''ARMED'', ''DET'', reference to the time delay);

(i) specially modified wooden or plastic boxes;

(j) unidentified powders or other putty-like substances; or

(k) carefully wrapped in plastic bags.

C.6 While the HOT protocol provides a useful starting point, it is not prescriptive. It is ultimately up to staff to use their judgement to decide whether an unattended item is suspicious or not.

C.7 Staff should seek immediate advice from a colleague or their supervisor if they are unsure about whether an item is suspicious or not.

Annex D – Quick reference security checklist

Item	Remarks	Action required
Introduction (Section 1)		
1.1 Do you have copies of the Bus and Coach Security DVD available?		
1.2 Do you use wider sources of security advice (e.g. CTSAs)?		
Organisational security culture (Section 2)		
2.1 Does your organisation encourage staff to respect common values and standards towards security?		
2.2 Does your organisation have ongoing effective personnel security measures in place?		
2.3 Are staff undertaking security related duties/tasks appropriately briefed/ trained?		
2.4 Does your organisation have contingency plans to deal with major incidents? Are these tested and practised?		
Handling threats and incidents (Section 3)		
3.1 Do you have a process in place for handling, reporting and recording bomb threats, and are you/your staff familiar with it?		
3.2 Are your staff aware of the BTP ''Marauding Active Shooter'' guidance?		
Security of buses and coaches (Section 4)		
4.1 Is the vehicle checked at end of route/turnaround?		

(*continued*)

Item	Remarks	Action required
4.2 Do you have a process for valuating and dealing with suspicious items/behaviour?		
4.3 Are the doors/windows secured when the vehicle is left unattended?		
4.4 Are passengers being prevented from boarding when vehicle not in service or driver not present?		
4.5 Are tickets being checked prior to passengers boarding or re-boarding?		
4.6 Are drivers/crew responsible for loading/unloading passenger baggage?		
4.7 Is there a process in place for dealing with luggage that appears suspicious or is handled suspiciously?		
4.8 Are there onboard passenger security announcements/information displayed?		
4.9 Is CCTV fitted onboard?		
4.10 How long are recordings retained?		
4.11 Is there a robust CCTV maintenance system in place?		
4.12 Are internal/external livery and markings removed?		
4.13 Are destination blinds, radio and access control systems removed?		
Security at bus and coach stations, termini and interchanges (Section 5)		
Areas of concealment		
5.1 Are all possible small concealed/ hidden from view areas removed or reduced?		
5.2 Are they checked frequently?		
5.3 Are security features designed into station/termini/stops?		

(*continued*)

Item	Remarks	Action required
Access control		
5.4 Are all doors to non-public areas locked or subject to access control?		
5.5 Are keys/access codes kept in a secure place?		
5.6 Are access codes changed regularly?		
5.7 Is the movement of vehicles (other than buses and coaches) controlled?		
5.8 Is there a process in place for dealing with illegally parked or suspicious vehicles?		
5.9 Are visitors/contractors required to report to the station manager or other responsible person to sign in and provided with an ID pass?		
5.10 Are visitors given a security briefing?		
5.11 Are there procedures in place for reporting suspicious behaviour?		
Patrolling public areas		
5.12 Is there a plan in place for regular patrols of public areas?		
5.13 Are patrols/search regimes changed regularly so that they cannot be monitored/learnt by those undertaking hostile reconnaissance?		
5.14 Is there a record of patrols?		
5.15 Are seals on locked doors checked?		
5.16 Is there a process in place for evaluating and dealing with suspicious items?		
Waste management		
5.17 Are litter bins of an IED resistant or clear plastic sack design?		

(*continued*)

Item	Remarks	Action required
5.18 Are litter bins emptied frequently?		
5.19 Are litter bins monitored by CCTV?		
5.20 Are large bulk waste containers stored in secure non public areas?		
5.21 If not stored away from public areas, are large bulk waste containers able to be locked, emptied regularly and CCTV monitored?		
Bicycles		
5.22 Are bicycle racks/lockers positioned away from crowded areas? Are they covered by CCTV?		
5.23 Are keys to lockers controlled and can staff access spare keys?		
Equipment boxes		
5.24 Are equipment boxes kept shut and secured?		
Public toilet facilities		
5.25 Are public toilets included in searches?		
Post boxes		
5.26 Are post boxes kept closed when not being emptied?		
Tenants and cleaners		
5.27 Do you have regular security meetings with tenants/cleaners/bus and coach operators?		
5.28 Are your tenants/cleaners security briefed?		
Passenger security awareness measures		
5.29 Are there passenger security announcements, or information displayed?		

(*continued*)

Item	Remarks	Action required
CCTV		
5.30 Is CCTV fitted and monitored?		
5.31 How long are recordings retained?		
5.32 Are all sensitive areas covered by CCTV cameras?		
5.33 Is there a robust maintenance system in place?		
Left luggage		
5.34 Are bags searched/screened before being stored?		
5.35 Do you have a process in place for reporting suspicious persons/bags?		
Car parks		
5.36 Are public car parks monitored and is there a procedure for dealing with suspicious vehicles?		
Security of depots and maintenance facilities (Section 6)		
6.1 Is the site perimeter secured with fencing/walls to keep intruders out?		
6.2 Are access control measures in place at all site entrances to prevent unauthorised access?		
6.3 Are CCTV cameras in place and monitoring/recording sensitive areas of the site?		
6.4 Are buses/coaches on site secured when not in use/undergoing maintenance work?		
6.5 Are vehicles searched before leaving the depot to enter service and again on returning, and is there a search recording system in place?		

Annex E – Glossary of terms

Active Shooter Scenario/Marauding Active Shooter means an attack using firearms, involving either a group or a lone shooter.

Bicycle/Cycle Locker means an enclosed structure provided for the storage of bicycles (whether singly or in bulk).

Bicycle/Cycle Rack means a device for the storage of bicycles that is of open construction and any bicycle placed in the rack is clearly visible.

Bomb Threat means a communication, anonymous or otherwise, which suggests that the safety of a bus/coach, station, other bus/coach premises or person may be in danger from an explosive or other such device that contains a harmful gas, chemical or biological substance.

BTP means the British Transport Police.

Bulk Rubbish Container means a large, rigid container (including wheelie bins and skips) for the storage and disposal of bagged and bulky waste items.

CPDA means a police Crime Prevention Design Advisor.

CPNI means the Centre for the Protection of National Infrastructure, the Government authority that provides security advice to businesses and organisations across the national infrastructure.

CTSA means a police Counter Terrorism Security Advisor.

Device includes, for the purpose of this guidance, all types of explosive, incendiary, chemical, biological, radiological or nuclear devices.

DfT means the Department for Transport.

HOT protocol means the procedure devised by BTP and promoted by NaCTSO to assist in determining whether an unattended item is lost property or something more suspicious.

IED means Improvised Explosive Device.

Left Luggage means any item deposited by a member of the public at a storage facility provided at a station (whether or not it is provided by the owner or operator).

NaCTSO means the police National Counter Terrorism Security Office.

Non-public Area means the areas of a station to which the public do not generally have access or to which they do not normally have access in the absence of supervision by a member of staff. Only members of staff or those contracted to provide services to buses, coaches, stations, buildings or machinery would ordinarily be expected to need access to those areas.

Open for Service in relation to any station shall be the earliest time in a day when a bus or coach at the station is available lawfully to be boarded, tickets are offered by members of staff for sale at ticket counters, or a bus or coach carrying passengers arrives.

Operator in relation to a station, means the person having the management of that station for the time being.

Owner in relation to a bus/coach station, means any person:

(a) who is the owner of, or who has any right over or interest in, the station; and

(b) whose consent is needed to use the station by any other person

Security Awareness Message means a message that makes the bus and coach travelling public and others using bus and coach facilities aware of and vigilant towards potential security threats affecting buses, coaches and stations.

Security Incident means any incident of a security nature where:

(a) the police are called and:
  (i) a full or partial evacuation of a station/bus/coach is required before the incident is resolved; or
  (ii) the initial police responders are unable to resolve the incident and call on further specialist assistance, such as Explosive Ordnance Disposal Officers, to resolve the incident; or
  (iii) the incident is resolved, but remains the subject of further police investigation; or

(b) police confirm the incident as an attempted or actual attack; or

(c) any security related incident which attracts media interest, even if it would not be one requiring notification in line with i) to iii) above; and

(d) any discovery of firearms, ammunition, or other weapons; and

(e) any incidents of unauthorised access, or attempted unauthorised access, to non public areas; and

(f) bomb threats; and

(g) any discovery of explosive devices, component parts of explosive devices, or articles having the appearance of such.

Security Staff in relation to any station means a member of staff who is engaged to provide security services to that station.

Station means any bus or coach station, terminus or interchange.

Suspicious Item means any thing that would be perceived by a reasonably prudent person, whether because of its physical characteristics, placement, or for any other reason, as of a kind that ought to be investigated by a person with security responsibilities.

Suspicious Behaviour means any behaviour that would be perceived by a reasonably prudent person as of a kind that ought to be investigated by a person with security responsibilities.

Threat Level means the level of threat the UK faces from terrorism at any given time.

Training Plan means a written document developed and maintained by a station/bus/coach operator which describes the type of security training that should be undertaken to ensure staff are aware of their security responsibilities and how to respond appropriately.