Department for Transport

Bus and Coach Security

Recommended Best Practice

Third edition

Moving Britain Ahead

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. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If bus and coach operators 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.gov.uk/dft
General enquiries: https://forms.dft.gov.uk

Contents

Section 1 – Introduction

Background

1.1 This guidance has been developed to support and promote the bus and coach industry in devising and maintaining a range of best practice security measures to protect against acts of violence, especially terrorism. It replaces the 2012 second edition and covers basic and enhanced security measures for:

- Building and embedding a security culture;
- Personnel security;
- Stations, termini and depots;
- Vehicles; and
- Generic security issues.

1.2 Following this guidance will strengthen counter terrorist security, reassure passengers and increase public confidence in using bus and coach services and facilities generally. It also has benefits in helping to reduce the risk of crime and anti-social behaviour.

1.3 The principles underpinning the advice throughout are:

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

How to use this guidance

1.4 This guidance is for bus and coach operators and owners/managers of bus and coach stations and depots.

Sections 1 to 3 - relevant to all;

Section 4 - relevant to bus and coach vehicle operators;

Sections 5 and 6 - relevant to bus and coach station and termini operators/owners, and

Section 7 - relevant to bus and coach depot operators/owners;

1.5 The Department for Transport (DfT) has also produced a Bus and Coach Security DVD which highlights basic security measures that bus and coach operators can put in place. It is intended as a training aid that can be used either to complement this Bus and Coach Recommended Best Practice Guidance or be shown independently to relevant personnel to raise awareness and encourage them to follow the suggested security procedures. Realistic scenarios are reconstructed with practical and straightforward messages.

Sources of advice, sharing awareness and further guidance

1.6 Other sources of advice, include:

- The Centre for the Protection of National Infrastructure (CPNI)'s booklet *Protecting Against Terrorism* offers general protective security advice for businesses and other organisations[1].
- Local authorities prepare emergency planning guidance as a requirement under the Civil Contingencies Act 2004 and may be able to provide assistance on some aspects (e.g. contingency planning). They can also assist if bus and coach operators have concerns regarding the positioning of street furniture such as litter bins or cycle racks.
- The CPNI and National Counter Terrorism Security Office (NaCTSO) websites which provide a variety of advice and guidance, including awareness of terrorism, physical security and personnel security[2] .
- Local police forces have expert Designing Out Crime Units, Designing Out Crime Officers (DOCOs) and Counter Terrorism Security Advisers (CTSAs) – all of whom are a good source of free security advice and assistance.
- For bus stations adjoining railway stations, contacting the railway station manager to discuss mutually beneficial security measures.
- Sharing best practice with other transport operators, infrastructure owners and managers in close proximity to you.

1 https://www.cpni.gov.uk/system/files/documents/5a/c9/Protecting-Against-Terrorism.pdf
2 https://www.gov.uk/government/publications/crowded-places-guidance

Terrorism threat levels

1.7 Details of the current UK national threat levels can be found on the MI5 Government website[3]. DfT Land Transport Security and the British Transport Police (BTP) CTSAs can also provide further information where appropriate.

There are 5 levels of threat:

- LOW - an attack is unlikely;
- MODERATE - an attack is possible but not likely;
- SUBSTANTIAL - an attack is a strong possibility;
- SEVERE - an attack is highly likely;
- CRITICAL - an attack is expected imminently.

1.8 Threat levels do not have an expiry date, and can change at any time as different information becomes available to security agencies.

DfT contact details

1.9 Please contact DfT's Land Transport National Security Division for further enquiries on bus and coach security or to request the free of charge Bus and Coach Security DVD at:

landsecurity@dft.gov.uk

or

Great Minster House, 33 Horseferry Road, London, SW1P 4DR

3 http://www.mi5.gov.uk/threat-levels

Section 2 – Organisational security culture

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

2.2 CPNI and NaCTSO have produced guidance[4] on building an organisational security culture and personnel security measures. This is designed to help organisations manage the risk of staff or contractors exploiting their legitimate access to premises, information and staff for unauthorised purposes.

Building and embedding a security culture

2.3 Senior management should develop a security culture within their organisation to encourage staff to adopt common security values and standards.

2.4 Security awareness amongst staff – staff vigilance when conducting everyday routines, for example, is an essential part of an organisation's security protection e.g. when cleaners undertake their operational duties, they should be able to identify suspicious items using the HOT protocol. Staff training, including regular drills and internal communications, plays 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 areas or faulty locks are not 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 is a system of policies and procedures that seeks to manage the risk of staff exploiting their legitimate access to an organisation's

4 https://www.gov.uk/government/publications/crowded-places-guidance

assets for unauthorised purposes. This is also known as the “insider threat”. The insider threat could come from disaffected staff or those that have been radicalised who might chose to carry out crime, terrorism or espionage. When consistently applied, personnel security measures not only reduce operational vulnerabilities but also help build a security culture at every level of an organisation.

2.8 A first step in developing good personnel security practices is to complete a personnel security strategy. This helps to identify risks and develop proportionate mitigations. Although many organisations regard personnel security as an issue that is resolved during the recruitment process through pre-employment checks, 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 management attitudes and relationships. Personnel security should also include a formal process for managing staff leaving the business.

2.9 CPNI promotes an Insider Threat Programme framework that covers the seven key elements shown below. Information on the key elements of personnel security can be found on the CPNI website[5].

- Governance and Leadership;
- Insider Risk Assessment;
- Pre-Employment Screening;
- Ongoing Personnel Security;
- Monitoring and Assessment of Employees;
- Investigation and Disciplinary Practices, and
- Security Culture and Behaviour Change.

2.10 Personnel security policies and processes should be integrated with existing physical and cyber security measures. Personnel security should take into account a company’s workforce, contractors (including the supply chain) and visitors.

Security training

Who should receive security training?

2.11 Staff (e.g. drivers, cleaners, and security staff) should, as a minimum, be briefed on security at regular intervals and receive appropriate training to ensure they are aware of any current issues relevant to them, their security responsibilities, and how to respond to an attack appropriately. This will help build

5 https://www.cpni.gov.uk

a security culture where the right security behaviours are adopted. The NaCTSO Crowded Places Guidance[6] also provides personnel security training and good practice.

What should security training include?

- **Security checking a bus or coach;**
- **Passenger luggage reconciliation;**
- **Searching or patrolling a station or other public area;**
- **The searching or screening (by hand, x-ray or using alternative detection equipment) of baggage being placed in a left luggage or lost property facility;**
- **Incident reporting;**
- **What to do in the event of an incident;**
- **Vigilance and controlling access into a non-public area; and**
- **Issuing passes for access to a non-public area.**

2.12 Training should also be given to those appointed as or acting in the capacity of:

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

6 https://www.gov.uk/government/publications/crowded-places-guidance

Training records

2.13 Where bus and coach staff are given specific training, we recommend that operators maintain training records which include:

- **The date that each member of staff 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 member of staff to confirm they received that training.**

Tenants and cleaners

2.14 Tenants and cleaners have their part to play in overall security and should follow the same basic principles and guidelines. We recommend that periodic meetings take place to discuss security issues, to involve all tenants and bus and coach operating companies using the station. Tenants and cleaners should be made aware of the importance of vigilance and given details of incident reporting procedures (who to report to and 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.

Administrative staff

2.15 Telephonists, receptionists, customer service staff, and any other administrative staff should be briefed about what to do in the event of an attack. The required response should be incorporated in staff instructions and staff should be issued with checklists on the steps to take if a threat is received. Supervisors should be made aware of how to respond and handle information about threats in accordance with local police advice – see Section 3.

Cyber Security

2.16 A cyber-attack has the potential to disrupt day-to-day operational activities and in the worst case scenario could put lives at risk or damage bus and coach assets. Embedding appropriate and proportionate cyber security measures will reduce the likelihood of an incident, and help minimise the impact and costs associated with any breaches.

2.17 The National Cyber Security Centre (NCSC) has been established to act as the Government's industry-facing centre of expertise on cyber security. The NCSC can assist with providing comprehensive cyber security advice and guidance, high-level threat intelligence and a 24/7 incident reporting function[7]. DfT has also produced some key principles for vehicle cyber security[8].

2.18 The Cyber Security Information Sharing Partnership (CiSP) is a forum for NCSC, industry and cross-industry collaboration and information sharing on cyber security[9]. Bus and coach companies should consider signing up to the CiSP which includes a transport and roads forum.

2.19 The EU Directive on Security of Network and Information Systems (NIS Directive[10]) provides a number of principles for the transport industry to follow to protect their operations. The indicators of good practice[11] may be used by coach and bus operators to self-assess their preparedness.

Further advice on Cyber Security can be found via the NCSC website, in particular the following advice should be considered:

- NCSC's 10 Steps in Cyber Security[12]
- NCSC's Cyber Essentials Scheme[13]
- NCSC's Securing Industrial Control Systems (guidance series)[14]

Contingency (Emergency) Plans

2.20 Contingency plans set out the steps an organisation should take to deal with any unplanned situation affecting its business which is likely to prejudice public safety or disrupt the ability to operate normally. Disruptive events cover a wide range of scenarios including terrorism, fire, adverse weather, loss of service (power and fuel etc.), loss of facilities and loss of staff. Every bus and coach operator, regardless of size, should develop a contingency plan against acts of terrorism. Issues to be considered include planning for the relocation of facilities and the directions given to passengers, staff and vehicles.

7 https://www.ncsc.gov.uk
8 https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles
9 https://www.ncsc.gov.uk/cisp
10 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
11 https://www.ncsc.gov.uk/guidance/indicators-good-practice
12 https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
13 https://www.ncsc.gov.uk/scheme/cyber-essentials
14 https://www.ncsc.gov.uk/guidance/security-industrial-control-systems

2.21 The main rules of contingency planning are:

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

2.22 Further information on developing risk assessments, responses and contingency plans is available from Local Authority Emergency Planning Officers.

Security exercises

2.23 Exercising enables organisations to:

- **Test existing plans, procedures and systems;**
- **Practise agreed roles with staff in a simulated and safe environment; and**
- **Evaluate plans and make any amendments as required.**

2.24 Exercises give everyone an opportunity to practise response arrangements with other parties who may be involved in an incident and to identify any gaps in contingency plans. Exercising should take place using a range of scenarios to ensure plans are sufficiently robust and staff are familiar with them. Where appropriate emergency services and local authorities should be involved in exercises. Bus and coach operators may also be asked to join in with exercises organised by the emergency services or other transport operators, and we would encourage bus and coach operators to participate. Local Authority Emergency Planning Officers can help bus and coach operators identify the correct contacts.

Section 3 – Handling threats and incidents

Key actions:

- **Print out the Threat Report Form (Annex B);**
- **Put the Threat Report Form in a prominent place that is easily accessible to staff, and store electronically;**
- **Brief staff who may receive a threat call on how to respond including the use of the Threat Report Form; and**
- **Use the Marauding Active Shooter Guidance (Annex C) to brief staff and the NaCTSO Crowded Places Guidance 2017 to help mitigate the threat and help make bus and coach stations and depots less vulnerable to attack.**

Received threats

3.1 Threats may be received or discovered by bus, coach, station and depot staff or anyone else connected with bus or coach operations. This also applies to administrative staff (see paragraph 2.15). Most threats are made by telephone, and may be received directly from the people issuing the threat or through intermediaries (e.g. the media and press agencies etc.). It may also be a recorded message or communicated via a third party, i.e. a person or organisation unrelated to the intended victim and identified only to pass on the message. With the advent of new technology and social media however, the bus and coach industry needs to be able to respond appropriately. As well as social media, this could be emails to general enquiry mail boxes, website 'Contact Us' pages, or text message inquiry services. No matter how implausible the threat may seem, recipients should try to obtain as much information as possible to help assess it and identify the person(s) issuing it. Whilst threats are usually hoaxes intended to cause alarm, disruption, fear or a nuisance, they must be taken seriously and assessed properly, as some may be genuine and precede a terrorist or criminal act. In the first instance, we suggest bus and coach operators seek advice from local police on how to handle any threats received.

3.2 Any recipient of a call or message that includes a threat should complete the Threat Report Form at **Annex B** (which is based on the standard police threat report form) and pass 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 administrative, customer service and sales staff), or discover a threat (such as cleaners or station patrol staff), should, on taking up their duties, be briefed on the possibility of receiving a threat message and the actions required in response. Supervisors should similarly be aware of what to do and of the need immediately to relay information to the police about any threat received. See Section 2 – Organisational security culture.

Firearms and knife incidents

3.3 NaCTSO has developed guidance giving advice on what to do in the event of a marauding terrorist firearms or knife attack affecting the network, whether by a co-ordinated group of terrorists or a lone actor. This is not a transport or modal specific issue as it concerns any crowded place where people may gather.

3.4 The parts of the guidance most relevant to the bus and coach industry are offered at **Annex C.** Further advice on keeping safe in the event of a marauding firearms or knife attack can be found via the NPCC website[15].

Chemical and noxious substance incidents (including unpleasant/unusual odours)

3.5 It is not uncommon for unusual or unpleasant odours to be detected inside or in areas near to buses, coaches, stations and depots. These are usually due to non-malicious activities or infrastructure faults (e.g. blocked drains, vehicle fumes or could be linked to anti-social behaviour). The use of chemical agents for malicious purposes however has the potential to put lives at risk.

3.6 If staff detect or are made aware of unusual or unpleasant odours, they need to consider the following:

- Could they be linked to recent cleaning activity, painting or maintenance work?
- Have they been noticed by staff on other occasions?
- Is there an obvious source (e.g. blocked drains, bus or coach exhaust fumes etc.)?
- Could an odour be from elsewhere (e.g. a nearby factory, road resurfacing, a bonfire etc.)?
- Could the odour be linked to anti-social behaviour (e.g. the malicious use of a stink bomb, a release of irritant spray)?

15 http://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttackStaySafe.aspx

3.7 In the event of a potential release of a chemical or noxious substance, the first indications may be reports of people becoming unwell. The key assessment criteria that staff and supervisors should apply in these circumstances are:

- Are casualty numbers escalating?
- Are casualties in close proximity to each other?
- How many people in the immediate area appear unaffected and are not displaying similar symptoms?
- Is there an obvious explainable cause for the casualties?

3.8 If casualty numbers are escalating, or if significant numbers of people are affected the following actions should be taken:

Key actions:

- **Report incident to relevant personnel (e.g. supervisor, facility manager, first aider and emergency responders);**
- **Do not put yourself or other bus and coach operators at risk;**
- **Always evacuate externally into fresh air;**
- **Prevent further people from entering the area.**

3.9 In the event of a chemical (including acid) attack, the first indication may be reports of victims suffering with subsequent injuries. The key actions should be to:

- **Report the incident to relevant personnel (e.g. supervisor, facility manager, first aider, emergency responders including the police) and follow their instructions;**
- **Evacuate from the affected area;**
- **Remove (where reasonably possible) any soiled or contaminated clothing;**
- **Apply first aid assistance (e.g. wash chemical (acid) agent with water);**
- **Make every effort to obtain full details from witnesses – especially immediate contact details – so that the police can speak directly to them and ask further questions if required.**

3.10 NaCTSO has developed further best practise security guidance[16] on what operators should do in the event of a chemical attack.

16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf

Section 4 – Security of vehicles

4.1 Passengers embark and alight freely, at approximately 400,000 bus and coach stops around the country. Simple measures can enhance security, deter attacks and reassure passengers.

Key actions:

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

Checking vehicles

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

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. On the railway network, the "**HOT**" protocol (at **Annex D**) is used to assess left objects.

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 bus and coach stations, termini and interchanges). Operators should therefore have discussions with their local police force to establish a system to enable unattended items to be reported and dealt with appropriately by their staff.

Securing vehicles

4.5 Whenever vehicles are left unattended (e.g. at the start and end of a journey, during a comfort break or whilst parked at termini, depots or stations),

drivers should ensure that all the doors and windows are closed. Where possible, passenger doors and baggage holds should be locked and, if appropriate, windows secured. This is to protect against someone entering the vehicle and leaving an item on board or taking the vehicle and potentially using it as a weapon.

4.6 Measures to prevent vehicles being taken by terrorists and used as a weapon include:

- **Vehicles should not be left unattended at the roadside with the ignition running;**
- **Ignition keys should not be left in the vehicle whilst the driver is not present;**
- **Alternative security measures should be considered for vehicles not requiring an ignition key;**
- **Security measures should be put in place at bus and coach stations to prevent unauthorised access to vehicles, and**
- **Drivers and/or bus and coach operators should report any concerns about unusual behaviour that occurs on or close to their vehicle.**

4.7 NaCTSO has developed general advice around the 'vehicle as a weapon' threat as part of their guidance (refer to page 67 of their advice) on protecting crowded places. This advice can be found via their website[17]. Where permanent physical security measures are being considered to mitigate this type of attack, bus and coach operators should seek specialist advice from CTSAs within their local police force.

Control of passengers boarding and leaving

Buses

4.8 Passengers should only be permitted to board buses and coaches when the driver is present and after a vehicle security check has been completed.

17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf

Coaches

4.9 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, until loading has been completed. If a coach makes a stop en-route (e.g. at a service station) the driver should satisfy him/herself that the correct passengers are re-boarding, perhaps by asking them to re-present their tickets. These measures will both help to increase security and reassure passengers.

Luggage reconciliation on coaches

4.10 Coach drivers, or any other member of the coach crew, where possible, should be responsible for loading and unloading all items of passenger baggage. Procedures should be developed to minimise the risk of someone placing an item in the baggage hold without boarding the coach, or of a disembarking passenger leaving baggage behind.

4.11 Reconciling passengers and luggage should:

- **Act as a deterrent to potential terrorists;**
- **Give coach crew an opportunity to visually check baggage on loading and identify any unusual behaviour. Special attention should be paid to any luggage that appears suspicious or is handled in such a way as to raise suspicions;**
- **Reassure passengers that the coach operator has appropriate security measures in place; and**
- **Minimise the risk of baggage items being left behind and any associated delays this may cause.**

4.12 It is important that staff know what to do and who to report their concerns to should they notice someone behaving unusually or have concerns about any suspicious items.

Security awareness messages for passengers

4.13 Security awareness messages are very useful in promoting vigilance and providing reassurance to passengers. Security posters should be displayed inside vehicles reminding passengers not to leave their bags unattended and of what to do if they find an unattended or suspect package or spot unusual behaviour, usually by reporting to a member of staff or a police officer. Where buses and

coaches are fitted with electronic messaging, TV screens, and public address systems these can also be used to disseminate security messages.

CCTV on vehicles

4.14 CCTV has useful deterrence and investigative 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.). Other 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.

The relevant code of practice advice on CCTV surveillance is available via the Information Commissioner's Office (ICO) website[18]

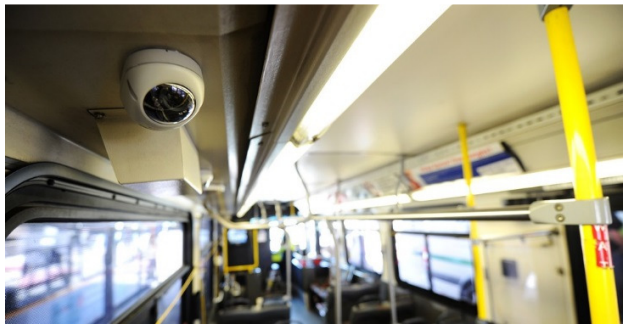

Figure 2 – CCTV on a bus

4.15 CCTV systems should be able to quickly export video and stills onto a removable storage medium, such as a CD, DVD or USB flash drive, 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.

4.16 Recordings should be retained for 31 days before the recording media is reused, and made available to police on request. A control log should be maintained to provide a record should CCTV recordings be required by the police or other agencies.

4.17 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

18 https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

identified and repaired quickly. If current CCTV systems are to be replaced or new ones installed, digital systems should be considered. Further information can be found on the CPNI website[19].

Disposal of vehicles

4.18 Prior to disposal or sale to third parties, all vehicles should have their entire internal and external livery and other markings removed, along with destination blinds and other equipment (e.g. radio and access control systems) to avoid potential use by others for malicious purposes. Electronic displays should be cleared and any hand-held units used for updating bus destination data, should be kept separate from vehicles in storage.

Security enhancements

4.19 For a summary of Security enhancements see **Annex A.**

19 https://www.cpni.gov.uk/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 are a potential terrorist target. Simple security measures can help to create a controlled environment which will act as both a deterrent and provide reassurance to customers.

- **Key actions:**
- **Remind passengers not to leave their luggage unattended and advise them to report unattended/suspect packages or unusual behaviour to staff or the police;**
- **Fit locks/tamper proof seals to cupboards/equipment boxes in public areas;**
- **Keep areas clear and tidy; see what "clutter" bus and coach operators can do without (this approach should not be applied to existing Hostile Vehicle Mitigation measures or those elements of street furniture that can help to deter a "vehicle as a weapon" attack against predictably crowded spaces); and**
- **Review bus and coach operator litter management arrangements.**

Areas of concealment

5.2 Some bus and coach stations were designed and built without security features and may 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 such areas, measures can be taken to reduce them, including:

- **Location of equipment – where possible, any grit bins, vending machines or other equipment boxes should be flush to walls so that nothing can be hidden behind or to the side of them; 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 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. Fitting machines back to back, or on legs with large gaps underneath, can reduce the opportunity to conceal items. Planters should be designed to make it impossible to hide anything underneath and planting should not be so dense that it hinders searches (e.g. well maintained environments have been found to be safer and more secure).

5.5 DfT's Security in the Design of Station (SIDOS) Guide[20] provides further detailed design advice and although it is targeted at railway stations, it is also applicable more generally to other public transport facilities.

Other sources of design guidance are

- Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation[21]; and

- Protecting Crowded Places: Design and Technical Issues[22]

Access Control

Non-public areas

5.6 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 between public and non-public areas should be kept locked or controlled to prevent unauthorised access. This will also minimise areas that need to be searched and patrolled.

5.7 Ideally, door keys should be kept securely, 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. Codes

20 https://www.gov.uk/government/groups/land-transport-security-division
21 https://www.cpni.gov.uk/system/files/documents/40/20/Integrated%20Security%20Guide.pdf
22 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf

should be 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 Vehicles may pose a threat both as the instrument for delivering improvised explosive devices and being used as weapons in ramming attacks. The movement of vehicles, other than authorised buses and coaches, at bus stations and depots should be strictly controlled. Ideally, all other vehicle access should be prevented, but where this is unavoidable (e.g. delivery to a retail outlet and access to staff parking areas) appropriate access controls should be adopted.

- **For example:**
- **A parking permit system for staff and, where possible, for visitor and contractor vehicles;**
- **Monitoring retail delivery vehicles to ensure they do not stay in the station for longer than is necessary; and**
- **Pre-arranged deliveries only.**

5.9 Operators should consult their local police force to agree a system for reporting and dealing with suspicious vehicles, and liaise with them regarding evacuation plans.

Visitors and contractors

5.10 All visitors and contractors to a bus or coach station should be required to report to the station manager/reception to notify their arrival. It is good practice to ask visitors to sign-in, issue visitor passes and check they have a legitimate reason for their visit. 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 Visitors and contractors should be given a security awareness briefing along the following lines:

- **Where a pass is issued, it should be displayed prominently at all times while they are on the premises;**

- **If they have a vehicle parked on site, any work/parking permits should be displayed prominently in the windscreen;**
- **Remind them to be vigilant when on the premises and of what to do if they see a suspicious item or a person acting unusually;**
- **Instruct them to properly close all doors when leaving, particularly doors leading to non-public areas;**
- **Ask them not to allow anyone to "tailgate" into non-public areas;**
- **Ask them to secure their worksites and equipment on leaving.**

Unusual behaviour

5.12 Procedures for reporting any unusual behaviour to supervisors and police, should be developed and briefed to all staff.

Reporting bus and coach operators concerns

5.13 If someone is seen to be acting in an unusual manner, or if unusual behaviour has been reported by a member of the public, supervisors or staff should establish:

i. When the person was seen displaying the behaviour (e.g. are they threatening passengers now?; or did they board a service 5 minutes ago? etc.) and;

ii. Was there any time lapse between witnessing the behaviour and it being reported?

Every effort should be made to obtain full details from the witness – especially immediate contact details - so that the police can speak directly to them and ask further questions if required.

- **Key actions/outcomes:**
- **Members of staff should report any concern;**
- **Obtaining detailed information can be essential in triggering a proportionate, timely and effective response by the police; and**

- **All unusual behaviour reports, regardless of outcome, are assessed and acted upon if necessary. Any concerns will be taken seriously.**

Patrolling public areas

5.14 Regular patrols by uniformed staff are a good deterrent, help to reassure passengers, and can play an important part in finding unattended or concealed items and detecting unusual behaviour. Patrolling patterns should not be shared outside the organisation. Where possible, unpredictable patrols should be introduced. Staff should also be encouraged to engage with the public and look out for individuals loitering with no clear sense of purpose, or individuals attempting to avoid staff interaction. Whilst dedicated and regular security patrols are ideal, resources may not necessarily permit this.

5.15 Security checks can be shared between 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 duties and by ticketing or sales staff present 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 should be carried out on opening and throughout the time when a bus or coach station is in service and open to the public. It is recommended that checks are recorded. These checks may provide critical information when reviewing incidents, particularly when backed up by CCTV.

5.16 Managers of other organisations (tenancies etc.) occupying premises or carrying out business at the station should be involved. This can help to ensure that all parts of the bus or coach station security check area are properly covered and that effective lines of communication are established.

5.17 The following steps will support effective security checks:

- **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 or accessible electronic records 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 and emergency exits, etc.) to be covered;

- **Thoroughness –** Checks need to be sufficiently thorough in order to detect any unattended or concealed items. Staff should pay particular attention to areas that are not in clear public view such as low roofs,

emergency exits, toilets, 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 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 (e.g. stores) not in regular use should be checked that they are secured under lock and key. When this is not possible, 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.

5.18 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, for example the **HOT** protocol shown at **Annex D** and in the DfT Bus and Coach Security DVD.

Waste management

Litter and recycling 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 It is recommended that the design of the bin should consist of a clear plastic sack (tinted sacks are acceptable, provided the colour does not obstruct easy viewing of the contents), suspended from a metal hoop sack holder with integral bungee strap(s) to secure the plastic sack. They should not have a lid, unless rubberised. The hoops should be attached to concrete or brick walls, or a wooden or single section steel or stainless steel metal post. Consideration should be given to covering bins by CCTV so that the face of anyone placing an item in the bin would be seen.

Figure 3 - Clear plastic sack, unobstructed from view, suspended from a metal hoop sack holder and attached to a brick wall.

5.21 Small receptacles, e.g. for used tickets, cigarettes, chewing gum, may be provided so long as any aperture is only as large as is needed to put the intended item in.

5.22 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 and to ensure they do not become over-full; and
- Keep the number of bins to the lowest practicable level and monitor usage to identify those 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, fire hydrants or electrical equipment etc.

Bulk rubbish containers and compactors

5.23 Large bulk rubbish containers (including wheelie bins, compactors and skips) should be kept in secure non-public areas where possible. However, if they are to be located 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 locked, and covered by CCTV cameras.

Public toilet facilities

5.24 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 onto the cistern. If refurbishment of a public toilet facility is being considered, designs that reduce or eliminate areas of concealment are preferred. A local Designing Out Crime Officer (DOCO) will be able to advise you.

5.25 Sanitary waste receptacles and receptacles for baby changing should be a purpose designed product and should ideally have a restricted aperture and be as small as practically possible. They should be checked and emptied regularly.

Bicycles

5.26 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

5.27 Bicycle racks should be positioned with regard to the safety of people and facilities. It is good practice, where possible, to avoid placing them directly opposite station entrances, exits or evacuation routes and not directly next to large windows. Derelict and abandoned bicycles should be removed once adequate notice of removal has been given.

Bicycle lockers

5.28 Bicycle lockers (whether for storage or for bicycle hire) also bring associated security risks. As with bicycle racks, positioning can minimise those risks, and we encourage bus and coach operators to follow the recommended mitigation measures listed in paragraph 5.27. Lockers should be secured with a padlock and key or any other equivalent measure designed to prevent unauthorised access. Consideration should be given to how the police will be given access to check lockers at short notice in the event of a security incident or alert. Lockers with mesh sides or adequate vision ports (to permit good visibility of the interior during low

light conditions) sufficient to ensure that the whole locker interior can be inspected from outside without the need to open it, are preferable and can assist in checking. These measures have the added benefit of reducing opportunity for criminals to conceal stolen goods or drugs in bicycle lockers, reducing general crime rates and enhancing overall personal security for staff and the public.

Figure 4 – Bicycle lockers. Picture taken by Alex Sully.

Figure 5 – Bicycle lockers with adequate vision ports sufficient to ensure that the whole locker interior can be inspected from outside without the need to open it. Picture taken by Alex Sully.

Equipment boxes

5.29 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 or 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.

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 them. The opening should be kept as small as possible to limit the size of items posted to letter format.

5.31 Advice should be sought from your local DOCO if an increase in the number of post boxes at a station is being considered, particularly if the installation of post boxes taking items larger than standard letter or small packet size is a possibility.

CCTV

5.32 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.

5.33 Bus and coach operators may wish to consider liaising with other local organisations/operations (e.g. railway stations, local authorities etc.) to identify whether it would be beneficial to have compatible systems or whether their CCTV surveillance covers any part of the bus and coach operation to avoid duplication. It may be possible for bus and coach operators to agree the final positioning of their systems to ensure that there are no potential gaps in coverage.

Car parks

5.34 We recommend that public car parks are monitored to ensure that vehicles near to buildings are not left for longer than authorised. 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 the local police force.

Security enhancements

5.35 For a summary of Security Enhancements see **Annex A**.

Interchanges

5.36 For the purposes of counter terrorism security, we ask bus and coach operators to cooperate with other operators where a bus or coach station adjoins another transport mode. A number of railway stations are required by DfT to have a Station Security Committee, which provides a forum for discussion on security matters affecting the station. Railway station operators must invite all interested parties to attend these Committees. Where the location of bus and coach operations forms part of a larger complex, operators may be asked to take part in Action Counter Terrorism (ACT) campaign[23] protective security events run by your local police force CTSAs. These are good opportunities to ensure bus and coach operator policies and procedures complement those of neighbouring businesses and operators. We ask that bus and coach operators remain open to any such invitations and for their active involvement. This will support bus and coach operators in addressing the areas covered in this guidance, often at an early stage.

23 https://act.campaign.gov.uk/

Section 6 – Security of locker facilities at bus and coach stations

Lockers

6.1 The provision of lockers for public use at bus and coach stations may be sought for a number of reasons including for internet purchases (click & collect), luggage storage, and for mobile device charging facilities. Controls on their location (e.g. away from the most crowded areas) and arrangements for their security management should be put in place.

6.2 Elements to consider for security management of lockers include being located away from crowded parts of stations, and being under CCTV coverage so that they may be monitored in the event of a security incident. Staff should also have a means of accessing the lockers or enabling the police to do so, by arrangement with the locker provider, to be able to check their interior – for example in circumstances of a bomb threat.

6.3 Where lockers are available at a bus and coach station for internet purchases ('click and collect'), a facility for delivery/collection of private sales (i.e. those not coming from a controlled (branded) supply chain) should not be offered, unless the goods are searched by hand or screened by x-ray prior to arrival, or on receipt, at the bus and coach station.

Figure 6 – InPost UK (collect & return parcel locker service) at Victoria Coach Station

6.4 Security processes should also be in place to ensure that customers who wish to return items are known e.g. by them having completed a minimum of two

transactions with the locker provider/retailer, in order to give a level of assurance that they are a genuine customer.

6.5 Self-service lockers, which a person accesses through direct cash or card payment, such as lockers for mobile device charging or left luggage, or lockers provided free of charge (e.g. for storage of cyclists' personal possessions), present an obvious security risk. They provide an uncontrolled potential concealment opportunity for a terrorist device, or for use by criminals to conceal stolen goods or drugs. Ideally they should not be located in stations and certainly not near to crowded areas. Any consideration of installing these should be guided by a risk assessment by the station operator.

Figure 7 – Charge Box (Mobile device charging facility)

Staffed left luggage facilities

6.6 At staffed left luggage facilities bus and coach operators 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 dealt with in this way.

6.7 We recommend that searching be carried out by hand searching items of luggage and their contents, or screening by using x-ray equipment, 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.

6.8 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 suspicion. Where a customer refuses permission to search and screen items, staff should not accept these and should notify their local police force immediately.

Figure 8 – Left Luggage facility

Section 7 – Security of depots and maintenance facilities

7.1 Although depots and maintenance garages are not crowded public places in the same way as stations are, some common sense security measures can help to ensure that an item is not concealed on board a vehicle when 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.

Security controls

7.2 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 which should be in good repair and maintained to current standards;
- Access control measures at all entrances to prevent unauthorised access; and
- Measures to protect buses and coaches within the site (locking of vehicles, regular patrols, or CCTV cameras to detect and monitor any unauthorised access).

7.3 Staff vigilance at all times is key to ensure the reporting of unattended items and unusual behaviour. Systems for recording site patrols, monitoring and checking of visitors and vehicles should be established. Identification passes should be worn at all times.

Buses and coaches on site

7.4 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 should be made of the checks.

Security enhancements

7.5 For a summary of Security Enhancements see **Annex A.**

Annex A – Security enhancements – at times of increased threat

Section 4 – Security of buses and coaches

- Increase frequency of security checks on board buses and coaches;
- Tighten security controls of boarding passengers and luggage reconciliation on coaches;
- Increase the frequency of security announcements to passengers and display security posters;
- Deploy revenue control officers and other bus and coach staff to travel on the network, wearing hi-vis jackets; and
- Brief staff on the importance of vigilance and remind them how to report any concerns.

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

- Carry out more frequent and thorough security checks of public areas in a station;
- Remove litter bins or increase the frequency of bin checks;
- Close bicycle parking facilities within the station area or request that panniers are removed before bicycles are left;
- Introduce/increase the frequency of passenger security announcements and 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;
- Deliveries to be by prior appointment only. Details of supplier, vehicle and driver to be checked and recorded on arrival; and

- Brief staff on the importance of vigilance and remind them how to report any concerns.

Section 7 – Security of depots and maintenance facilities

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

Annex B – Threat Report Form

Threat Report Form – threats made by telephones, etc. or face-to-face

To be completed by/with the assistance of the information recipient

To be forwarded immediately to the supervisor

To be retained for 12 months

Other modes of communication. Threats received in writing or via email, social media, etc., should prompt a response/acknowledgement but must be reported to police and made available for inspection.

ACTIONS TO BE TAKEN ON RECEIPT OF A THREAT

1. Remain calm and talk to the caller
2. Note the caller's number if displayed on your phone
   threat:
3. If the threat had been sent via email or social media,
   see appropriate section below
4. If you are able to, record the call
5. Write down the exact wording of the

ASK THESE QUESTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Is this a one-off bomb threat or are there multiple threats?

9. Where exactly is the bomb threat now?

	Company	Location	Details (e.g. bus/coach number, route, destination)
Bus			
Coach			
Stop			

Station Terminus Other			

2. When is it going to explode?

10. What is your name?

3. What does it look like?

11. What is your address?

4. What does the bomb contain?

12. What is your telephone number?

5. How will it be detonated?

13. Are you a group or are you acting alone?

6. If moved? After departure ☐ In transit ☐ If opened? ☐

7. Did you place the bomb? If not you, who did?

14. What is the name of the group?

8. Why have you placed the bomb?

15. Record time completed:

INFORM SECURITY OR COORDINATING MANAGER

DIAL 999 AND INFORM POLICE

Name and telephone number of person informed:

Time informed:

Mobile Phone	Pay Phone	Private Phone	Internal Call	External Call

This part should be completed once the caller has hung up and the police/security/coordinating manager have all been informed:

Date and time of call:

Duration of the call:

The telephone number that received the call:

About the caller:

☐ Male ☐ Female ☐ Age ☐ Nationality ☐

☐ Child ☐ Teen ☐ Young adult ☐ Middle aged ☐ Old ☐ Unknown ☐

Threat language:

☐ Well-spoken ☐ Irrational ☐ Taped ☐ Foul ☐ Coherent

Caller's voice:

☐ Calm ☐ Slurred ☐ Lisp ☐ Crying ☐ Excited ☐ Rapid ☐

☐ Clear throat ☐ Stutter ☐ Deep ☐ Angry ☐ Disguised ☐ Laughter ☐

☐ Nasal ☐ Slow ☐ Loud ☐ Hoarse ☐ High Pitched ☐ Intoxicated ☐

☐ Rasping ☐ Pleasant ☐ Soft ☐ Rational ☐ Irrational ☐ Incoherent

☐ Deliberate ☐ Concerned ☐ Righteous ☐ Coherent ☐ Emotional ☐

☐ Obscene ☐ Other (please specify ☐

☐ Familiar (If so, who did it sound like?)

☐

☐ Accent (If so, what accent?)

☐

Other sounds:

☐ Street noises ☐ Motor ☐ PA System ☐ Office machinery ☐
TV

☐ House noises ☐ Clear ☐ Booth ☐ Animal noises ☐
Radio

☐ Voice ☐ Music ☐ Crockery ☐ Static ☐ Aircraft

☐ Factory machinery ☐ Other (please specify)

Remarks:

Any additional information/notes (i.e. person(s) appeared to have intricate knowledge of the industry/location/response):

Recipient's details (must be filled in):

Signature: _____ Print name: _____

Date: ____/____/____/ Position: _____ Phone Number: _____

Threat received at: _____ Time: _____

Form passed to Supervisor (name): _____

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1. Do not reply to, forward or delete the message
2. If sent via email, note the address
3. If sent via social media, what application has been used and what is the username/ID?
4. Dial 999 and follow police guidance
5. Preserve all web log files for bus and coach operators organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

Signature: _____ Print name:_____

Date: _____/_____/_____/

SAVE AND PRINT – HAND COPY TO POLICE AND SECURITY OR COORINATING MANAGER

Annex C – Marauding terrorist firearms and knife attack guidance

C.1 This guidance is intended to complement existing guidance, by addressing the scenarios that have emerged in recent terrorist attacks. “Marauding terrorist firearms and knife attack” covers all firearms or knife attacks, whether by a co-ordinated group of terrorists or a lone actor, against one or multiple targets. This style of attack is potentially attractive to any crowded area, so vigilance by managers and staff everywhere is important.

C.2 We are not asking bus/coach organisations or staff to put themselves in the line of fire. 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 as effectively as possible.

C.3 In briefing staff, or responding to staff concerns, bus and coach operators may like to explain:

“This guidance is not being provided in response to any specific threat intelligence. However, it is important that we consider potential 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.”

“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 like this raises, it will help bus and coach operators know the best things to do in the unlikely event of it happening.”

Bus and coach operators might also consider providing an overview of the current national threat level reported for terrorist attacks in the UK which is obtainable from the Security Service (MI5)[24].

C.4 The National Police Chiefs Council has produced a “Stay Safe” video which provides advice to the public on what actions they should take to stay safe in the event of a terrorist firearms attack[25].

24 http://www.mi5.gov.uk/threat-levels
25 http://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx

C.5 In the event of an attack on a vehicle or at a station consider these actions:

Run

- **Under IMMEDIATE ATTACK** – Take cover initially, but leave the area as soon as possible, putting distance between yourself and the attacker(s) and if it is safe to do so, e.g. if the attacker(s) are no longer a threat to you or others in your vicinity.

- **Nearby attack** – Leave the area immediately, if it is possible and safe to do so.

- **Evacuation** – Be aware of location and direction of threat and evacuate away from danger. Assist others in evacuating if it is safe to do so.

- **Leave personal belongings behind** – Do not delay evacuation but, if possible, take a means of communication (i.e. mobile phone) to facilitate you giving and receiving 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.

Hide

The opportunities for passengers on a bus/coach to 'Hide' until there is an opportunity to run are very limited. Passengers should leave the area as soon as possible (i.e. 'Run') - when it is safe to do so.

Tell

Pass as much information to the **Police** as possible. **NEVER** risk your **own safety** or that of **others**.

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

• Is it a weapons incident?
• Exact location of the incident?
• Type of weapon – firearm, knife, sword, or machete?
• Moving in any particular direction?
• Number and description of attackers?

• What else are they carrying?
• Are they communicating with others?
• Number of casualties/people in the area?

Do not assume that others have already contacted the Police. Therefore contact them immediately by dialling 999, giving them the information shown above.

Using this information, the police will take the necessary action to ensure the right resources attend the scene so that assistance can be provided.

Use all **forms of communication** available to bus and coach operators – to inform staff and public of the danger.

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

C.6 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 staff and passengers from the gunmen.
- Officers may be armed and may point guns at staff and passengers.
- They may have to treat the public firmly.
- Follow their instructions; keep your hands in the air and in view.
- Avoid quick movement towards the officers and pointing, screaming or shouting.

Plan

Consider the following when planning for a marauding terrorist attack incident:

1. How bus and coach operators would communicate with staff, the public, the police and neighbouring premises etc.?
2. What key messages would bus and coach operators give in order to keep people safe?
3. Do you have the ability to secure key parts of the building to hinder free movement for the marauding terrorists?
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 the above into your emergency security planning and briefings.
6. Test emergency security plans to ensure they are robust and fit for purpose.

If bus and coach operators require further information then please liaise with your immediate Supervisor.

Annex D – Evaluating unattended items: The HOT protocol

D.1 **Introduction**. The HOT protocol has been used in the railway environment since the early 1990s and is reviewed regularly. It has been designed by the BTP to assist rail staff in determining whether an unattended item or bag found at a station is a genuine item of lost property or potentially something more suspicious. The **HOT** protocol has also proved effective in minimising delays. This protocol is equally applicable in the bus and coach sector and forms the basis of national advice provided by the National Counter Terrorism Security Office (NaCTSO). It is based on extensive research by BTP which highlights **the importance of answering three key questions when an item is discovered in a public space without an apparent owner**:

- **H**idden – Has the item been placed where it will not be seen easily or noticed as unusual?
- **O**bviously suspicious – Is its physical appearance odd? Has it been located in an unusual place? Are the circumstances of its discovery suspicious or unusual?
- **T**ypical – Is the item typical of what bus and coach operators would normally expect to find in the given location?

These factors must be considered together – ideally by someone familiar with the environment.

D.2 **Risk management response**. The initial evaluation (as informed by the answers to the three key questions shown above) will then inform the most appropriate risk management response; this will involve either:

a) An active decision to evacuate immediately – <u>because</u> the object has defined 'suspicious' characteristics and is believed to represent an immediate threat to life;

or

b) An active decision to examine the item more closely because it is not overtly suspicious (i.e. it has the characteristics of lost property, discarded rubbish etc.). This will involve looking inside the item, checking for its owner, reviewing CCTV, talking to anyone nearby etc.

D.3 It is difficult to define comprehensively how items might appear "obviously suspicious" from their external appearance alone. However, a hazardous item may display one or more of the following features: not all of which will necessarily be visible before it is examined more closely.

(a) External wiring linking components, such as: batteries; switches; timers and/or mobile telephones or exposed circuit boards.

(b) Wire passing from one 'package'/container to another, possibly including: specially modified wooden, plastic or metal containers or boxes.

(c) Items secured by plastic adhesive tape.

(d) Annotations (e.g. "ON", "ARMED", "DET" or a possible reference to the time delay).

(e) Unidentified 'powders' or other putty-like substances – Possibly carefully wrapped in plastic bags.

D.4 **Informed judgement**. Whilst the HOT protocol provides **a rational starting point for risk management decision-making**, it is not prescriptive. Ultimately it is up to staff to use their judgement, experience and knowledge of the environment in question to decide whether an unattended item is 'suspicious', or not, and whether immediate evacuation is necessary because an immediate threat to life has been identified. If doubt exists about an item's status, staff should seek immediate advice from a colleague or their supervisor. **REMEMBER** – a predictable 'precautionary' evacuation (i.e. one initiated before the presence of a hazardous item is confirmed) can be exploited by terrorists.

Reporting a confirmed suspicious item

D.5 The "Five W's" format should be used to report information to police:

- **What is it?** – What does the item look like?
- **Where is it?** – Are there any obstacles or nearby hazards that would prevent access? How close are people?
- **When was it found?** – Has it been moved since it was found? When was it known to have been absent?
- **Why is it suspicious?** – Can its discovery be linked to earlier suspicious behaviour or threats? Who has seen it? – Any witnesses should be asked to wait for the arrival of the police.

Annex E – Quick reference security checklist[26]

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?		
Item	**Remarks**	**Action required**
Organisational security culture (Section 2)		
2.1 Are your staff undertaking security related duties/tasks appropriately briefed/trained?		
2.2 Does your organisation have contingency plans to deal with major incidents? Are these tested and practised?		
Item	**Remarks**	**Action required**
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 terrorist firearms or knife attack" guidance?		
3.3 Have you considered measures to prevent vehicles from being taken by terrorists and used as a weapon?		

26 NaCTSO has a range of further checklists (see page 141 of their 2017 Crowded Places Guidance) which may be of benefit to operators.

Item	Remarks	Action required
Security of buses and coaches (Section 4)		
4.1 Is the vehicle checked at the end of route/turnaround stage?		
4.2 Do you have a process for valuating and dealing with unattended items or unusual behaviour?		
4.3 Are the vehicle doors/windows secured when the vehicle is left unattended?		
4.4 Are passengers being prevented from boarding when the vehicle is not in service or the driver is 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 being handled suspiciously?		
4.8 Is there on-board passenger security announcements/information displayed?		
4.9 Is CCTV fitted on-board?		
4.10 How long are CCTV recordings retained for?		
4.11 Is there a robust CCTV maintenance system in place?		
4.12 Are internal/external livery and markings removed when a vehicle is no longer in use?		
4.13 Are destination blinds, radio and access control systems		

cleared or removed when a vehicle is no longer in use?		
Item	**Remarks**	**Action required**
Security at bus and coach stations, termini and interchanges (Section 5)		
Areas of concealment		
5.1 Have all possible concealment opportunities or hidden from view areas been removed?		
5.2 Are they checked frequently?		
5.3 Are security features designed into stations/termini/stops?		
5.4 Have you referred to SIDOS when considering the security design of the bus stations/termini/stops?		
Access control		
5.4 Are all doors to non-public areas locked or subject to access controls?		
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 provide them with an ID pass?		
5.10 Are visitors given a security briefing?		

5.11 Are there procedures in place for reporting unusual 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 they cannot be monitored/learned by potential terrorists 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 that are unattended?		
Waste management		
5.17 Are litter bins of a clear plastic sack design to limit fragmentation?		
5.18 Are litter bins emptied frequently?		
5.19 Are litter bins monitored by CCTV?		
5.20 Are large bulk waste containers located in secure non-public areas?		
5.21 If located in 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 bicycle 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 security searches?		
Post boxes		
5.26 Are post boxes kept locked when not being emptied?		
Tenants and cleaners		
5.27 Do bus and coach operators have regular security meetings with tenants/cleaners/other bus and coach/transport operators?		
5.28 Are tenants/cleaners security briefed on a regular basis?		
Passenger security awareness measures		
5.29 Are there passenger security announcements or is there security information displayed (posters)?		
CCTV		
5.30 Is CCTV fitted and monitored?		
5.31 How long are CCTV recordings retained?		
5.32 Are all sensitive areas covered by CCTV?		
5.33 Is there a robust maintenance system in place?		
Car parks		
5.34 Are public car parks monitored and is there a		

procedure for dealing with suspicious vehicles?		
Security of locker facilities at bus and coach stations (Section 6)		
Lockers		
6.1 Are any lockers in place for public use at bus and coach stations situated away from crowded areas?		
6.2 Are all self-service lockers located within an area covered by CCTV so they can be monitored in the event of a security incident?		
Item	**Remarks**	**Action required**
Security of depots and maintenance facilities (Section 7)		
7.1 Is the site perimeter secured with fencing/walls to keep intruders out?		
7.2 Are access control measures in place at all site entrances to prevent unauthorised access?		
7.3 Are CCTV cameras in place to monitor/record sensitive areas of the site?		
7.4 Are any buses/coaches on site fully secured when not in use/undergoing maintenance work?		
7.5 Are vehicles searched before leaving the depot to enter service and again on returning, and is there a search recording system in place?		

Annex F – Glossary of terms

Bicycle/Cycle Locker means an enclosed structure provided for the storage of bicycles (whether singularly 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 vehicle, station or other bus/coach premises 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.

DOCO means Designing Out Crime Officer.

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).

Marauding terrorist firearms/knife arrack means all firearms or knife attacks, whether by a co-ordinated group of terrorists or a lone actor, against one or multiple targets**.**

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.

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

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 bus, coach, station is required before the incident is resolved; or

  (ii) the initial police responders are unable to resolve the incident and call in further specialist assistance, such as the 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 noteworthy media or social media interest, or is considered to be likely to do so, or which is causing disruption to operations, should be reported to the DfT immediately, 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) any incidents of sabotage; and

(g) any persons exhibiting Unusual and/or Suspicious Behaviour;

(h) bomb threats; and

(i) 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 an item exhibiting unusual characteristics (appearance or placement) and for which ownership or a legitimate purpose cannot be established readily.

Unusual 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.

The 5 W's is a national initiative that can be used alongside the "HOT Protocol" to assist staff in assessing unattended items.

Vehicles includes buses and coaches.

Annex G – Summary of Sources

Section	Topic	Organisation	web link
Section 1	Protecting Against Terrorism security advice	CPNI	https://www.cpni.gov.uk/system/files/documents/5a/c9/Protecting-Against-Terrorism.pdf
	Awareness of terrorism and physical security	CPNI	https://www.gov.uk/government/publications/crowded-places-guidance
	DfT contact details	DfT	landsecurity@dft.gov.uk
Section 1 & Annex C	Threat levels	MI5 Government	https://www.mi5.gov.uk/threat-levels
Section 2	Personnel security	CPNI	https://www.cpni.gov.uk
	Cyber security information Sharing Partnership (CiSP)	NCSC	https://www.ncsc.gov.uk/cisp
	Key principles for vehicle cyber security	DfT/CPNI/Centre for Connected and Autonomous vehicles	https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles
	Cyber Security – NIS Directive on Security of Network & Information Systems	NCSC	https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
	Indicators of good practice	NCSC	https://www.ncsc.gov.uk/guidance/indicators-good-practice
	Cyber Security advice	NCSC	https://www.ncsc.gov.uk
	NCSC's 10 Steps in Cyber Security	NCSC	https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
	NCSC's Cyber Essential Scheme	NCSC	https://www.ncsc.gov.uk/scheme/cyber-essentials
	NCSC's Security Industrial Control Systems (guidance series)	NCSC	https://www.ncsc.gov.uk/guidance/security-industrial-control-systems

Section 3	Keeping Safe in the event of a marauding firearms or knife attack	NPCC	http://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttackStaySafe.aspx
Section 4	CCTV technological systems	CPNI	https://www.cpni.gov.uk/cctv
	CCTV surveillance - Code of Practice	Information Commissioner's Office (ICO)	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
Section 4 & 5	Protecting Crowded Places: Design and Technical Issues	CPNI/NaCTSO/HO	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf
Section 5	Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation	CPNI	https://www.cpni.gov.uk/system/files/documents/40/20/Integrated%20Security%20Guide.pdf
	Action Counter Terrorism (ACT) Campaign	NaCTSO	https://act.campaign.gov.uk/
Section 5	DfT/ Land Transport Security Guidance documents (including Security in the Design of Station (SIDOS))	DfT	https://www.gov.uk/government/groups/land-transport-security-division
Annex C	Stay Safe Video	National Police Chiefs Council (NPCC)	http://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx