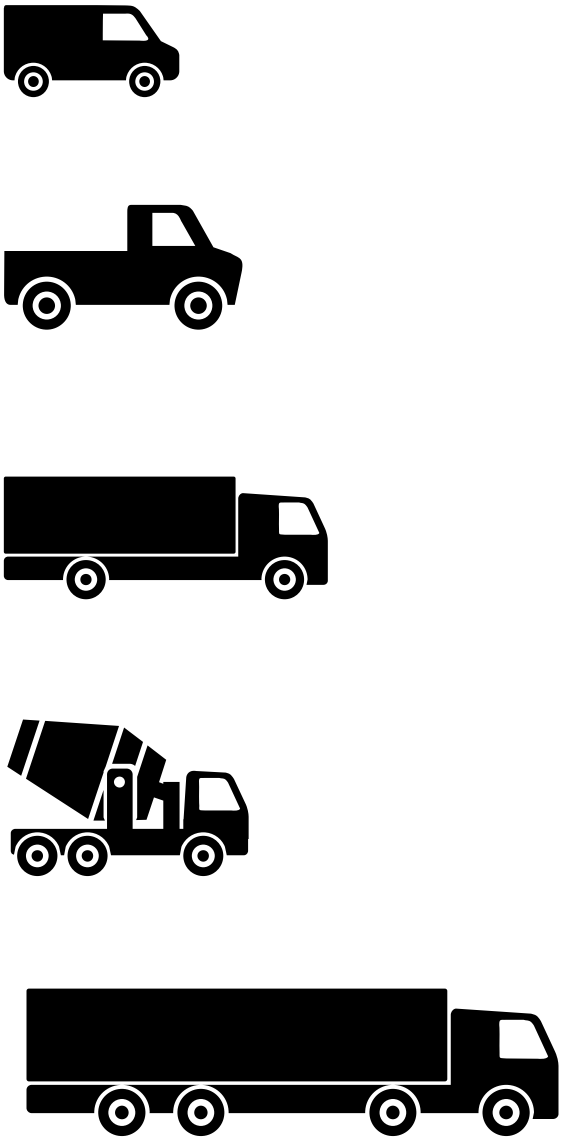
Department
for Transport

Vehicle as a Weapon: Best Practise Guidance for Commercial Vehicle Operators and Drivers



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 Commercial Vehicle operators and drivers 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

Section 2 – Security Culture

Section 3 – Site Security

Section 4 – Vehicle Security

Section 1 – Introduction

1.1 Purpose of this Guidance

This guidance has been developed to ensure Transport Operators are alert to the threat of Commercial Vehicles being used in Vehicle as a Weapon (VAW) attacks. It sets out simple steps Transport Operators should take to promote a good Security Culture in their organisation and help keep drivers, sites and vehicles secure. A 10-point Security Checklist (annex A) provides best practice for Commercial Vehicle drivers, to reduce the risk of their vehicles being stolen for use in an attack. The Checklist is designed to be kept in the vehicle cab.

Links to a wide range of more detailed official guidance are at Annex B.

1.2 What is a Commercial Vehicle?

For the purpose of this guidance, the term Commercial Vehicle applies to a vehicle designed to carry goods or materials rather than passengers.

1.3 What is a Vehicle as A Weapon attack?

A vehicle can be used as a weapon to injure and kill people. This is referred to as a ‘vehicle as a weapon attack’. VAW is a low complexity methodology requiring little or no training and is therefore within the capability of many individuals. Crowded public spaces provides targets for this type of attack. There are a range of online terrorist and extremist materials aimed at inspiring terrorists to carry out VAW attacks[1]. Lorries and vans pose a particular risk in VAW attacks because of their size and weight increasing the potential impact.

This is a real threat: there have been numerous VAW attacks in the UK and around the world in recent years killing and injuring hundreds of innocent people.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

Section 2 – Security Culture

2.1 What is a Security Culture?

The Centre for the Protection of National Infrastructure (CPNI), defines Security Culture as ‘a set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security[2].’ Security Culture is a collective attitude to security procedures and shapes individual behaviours. A strong Security Culture will support a company’s Corporate Social Responsibility (CSR) duties to protect the public, its customers and assets.

The benefits of an effective Security Culture according to CPNI are[3]:

- **A workforce that are more likely to be engaged with, and take responsibility for, security issues**
- **Increased compliance with protective security measures**
- **Reduced risk of insider incidents**
- **Awareness of the most relevant security threats**
- **Employees are more likely to think and act in a security conscious manner**

[2] https://www.cpni.gov.uk/developing-security-culture
[3] https://www.cpni.gov.uk/developing-security-culture

2.2 Security Culture in your organisation

Using the CPNI 5E's framework (Educate, Enable, Shape the Environment, Encourage the Action and Evaluate the Impact) an organisation can embed and sustain security behaviours within their workforce. The CPNI 'Embedding Security Behaviours: using the 5Es Framework' document provides guidance on how to implement the 5Es within an organisation[4].

2.3 Suspicious behaviour

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 and those not wearing those should be challenged (see Visitors and Contractors- Section 3).

Getting your organisation to behave in a 'security savvy' way, to be vigilant and to report suspicious activity can help your chances of detecting people with hostile intentions, as well as deterring them. Employees can be a massive enhancement to other existing elements of protective security[5].

2.4 Insider Threat

Insiders with access to your processes and assets can be a particular source of threat. The risks posed by the insider threat can be lessened by carrying out thorough pre-employment checks and by having a strong Security Culture[6].

CPNI defines an insider as a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes[7]. An insider could be a full time or part-time employee, a contractor or even a business partner. An insider could deliberately seek to join your organisation to conduct an insider act, or may be triggered to act at some point during their employment.

2.5 Pre-employment checks for all employees

Robust pre-employment checks for all employees can mitigate the insider threat by [8]:

[4] https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf
[5] https://www.cpni.gov.uk/optimising-people-security
[6] https://www.cpni.gov.uk/personnel-and-people-security
[7] https://www.cpni.gov.uk/reducing-insider-risk
[8] https://www.cpni.gov.uk/pre-employment-screening

- **deterring applicants who may wish to harm your organisation from applying for employment**

- **detecting individuals with an intent to harm your organisation at the recruitment/application phase**

- **denying employment to individuals intending to harm your organisation, and deny employment in roles for which the applicant is unsuitable.**

It is recommended that you use British Standard 7858 (or equivalent) for security screening of employees[9]. BS7858 sets out recommendations for the security screening of individuals to be employed in an environment where the security and/or safety of people, services, personal data or property is a requirement of the employing organisation’s operations or where such screening is in the public or corporate interest. [10].

2.6 Pre-employment Checks for Drivers

The National Counter Terrorism Security Office (NaCTSO) recommend that the following steps are taken when employing drivers[11]’:

• check a driver’s references and previous employment history (minimum of five years and up to ten years).

• speak to previous employers (do not rely on phone numbers given by the driver).

• inform applicants that false details on application forms may lead to dismissal.

• check driving licenses are valid and look for endorsements before you employ someone, and then at six-monthly intervals afterwards. Drivers should tell you of any changes to their license.

• check if the applicant has any prosecutions pending or is waiting for sentencing by a court.

[9] https://shop.bsigroup.com/ProductDetail?pid=000000000030237324

[10] https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf

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

• for agency drivers, ensure that the agency has carried out all of these checks including criminal records checks.

• use only reputable agencies that are affiliated with a recognised UK trade organisation.

2.7 What is ACT?

Action Counters Terrorism (ACT) is the national campaign by National Counter Terrorism Policing which urges the public to act on their instincts to help tackle the terrorist threat.

The public already contribute intelligence to around a third of the most serious terrorism investigations. This new campaign reassures communities that they shouldn't be concerned about wasting police time or getting someone into trouble.

2.8 Reporting suspicious concerns

The message is clear - 'If you've seen or heard something that could suggest a terrorist threat to the UK do not ignore it, report it' by[12]:

- reporting suspicious activity to the police by calling confidentially on 0800 789 321 or at https://act.campaign.gov.uk/

- remaining alert so we can all play our part in defeating terrorism and keeping everyone safe.

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

[12] https://act.campaign.gov.uk/

Section 3 – Site Security

Security measures on site can help to create a controlled environment which will encourage a Security Culture amongst staff and act as a deterrent as well as protecting from theft and other criminal activity.

Organisations can consult their regional Counter Terrorism Security Advisor (CTSA) to agree a system for reporting and dealing with suspicious vehicles, and liaise with them regarding securing their sites[13].

Basic security measures can help to ensure that an item is not concealed on board a vehicle when in maintenance centres. Having clear signage in place can discourage unwanted access by vehicles and people.

Examples of site security actions[14]:

- **Staff should be vigilant and report any unauthorised or unattended items to the Transport Manager**
- **Staff should report any unusual behaviour to staff or the police;**
- **Staff should report any unauthorised access to premises to the Transport Operator or the Police;**
- **Fit locks or tamper proof seals to cupboards and equipment boxes in public areas;**
- **Access to operating centres should be controlled with appropriate security arrangements i.e. fences, gates, security codes**
- **Vehicle keys should be stored in a secure locker with security codes. Keys should not be left in vehicles.**

3.1 Visitors and contractors

All visitors and contractors visiting premises should be required to report to reception to notify their arrival. Visitors should sign-in, be issued visitor passes

[13] https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

[14] https://publications.europa.eu/en/publication-detail/-/publication/677076fa-fc01-11e7-b8f5-01aa75ed71a1/language-en

and 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.

Visitors and contractors should be given a security awareness briefing to include[15]:

- **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.**
- **Challenging others if they are not wearing a pass or are in an area where they shouldn’t be.**

3.2 Vehicle access at sites

The movement of any unauthorised vehicles on site should be strictly controlled and ideally prevented. If this is unavoidable, appropriate access controls should be adopted for example: a parking permit system for staff, visitor and contractor vehicles or allowing pre-arranged deliveries only.

3.3 Security controls

All sites with parked vehicles not in use should be subject to security controls. These include:

- **Physical access barriers around the site such as walls and fences which should be in good repair and maintained to acceptable standards;**
- **Access control measures at all entrances to prevent unauthorised**

[15] https://www.cpni.gov.uk/content/control-access

access;

- **Measures to protect vehicles on the site (locking of vehicles, regular patrols, or CCTV cameras to detect and monitor any unauthorised access).**

3.4 Operating Centres

The movement of vehicles, other than authorised, at operating centres should be strictly controlled. Ideally, all other vehicle access should be prevented, but where this is unavoidable appropriate access control should be adopted.

Transport Operators should consult their CTSA to agree a system for reporting and dealing with suspicious vehicles, and liaise with them regarding evacuation plans.

3.5 CCTV

CCTV is often one of the main stays of a modern security system. Its primary focus is to act as a detection and verification system for other security measures. CCTV can be a single or combination of systems and technologies to form the overall security solution. [16]

Most electronic detection systems assured by CPNI work on the five minute rule. This assumes that each part of a perimeter or sensitive asset is viewed by either a guard or CCTV once every five minutes. This limits the potential time for an unauthorised activity and forces an attacker to carry out a rapid attack, making them more likely to trigger an electronic detection system.

3.6 Unsecure Locations

It is not always possible for vehicles to be parked in a secure location on the road. A driver is a lone worker[17] and it is important they feel safe and secure whilst working.

If parking in an unsecure location[18], drivers should ask themselves:

- **Is your vehicle locked with windows closed? Do you have your**

[16] https://www.cpni.gov.uk/cctv
[17] http://www.hse.gov.uk/toolbox/workers/lone.htm
[18] https://publications.europa.eu/en/publication-detail/-/publication/677076fa-fc01-11e7-b8f5-01aa75ed71a1/language-en

keys on your person at all times?

- **Have you activated the vehicles security devices where applicable?**
- **Has anyone followed you, are you being watched?**
- **If possible, can you keep the vehicle in sight at all times?**
- **Is the area well lit?**
- **When returning to your vehicle, does it look the same as when you left?**
- **Are there any external factors that you could reasonably predict (eg. weather) that could disrupt your route?**
- **Does your Company know where you are parking?**
- **Are there unsecure parking areas recommended by others which they feel are safe and secure?**
- **Do not post your location on social media.**[19]
- **If you are approached or stopped by police only open the cab window after officers have showed their identification and alert your Transport Operator. If you suspect the individual is not a police officer keep the cab locked and do not get out the vehicle, drive to the nearest Police Station and call 101.**
- **Be mindful that the only public bodies with legal powers to stop you whilst driving are the Police, DVSA, Highways authorities such as Highways England and those granted CSAS powers by the Police.**

Section 4 – Vehicle Security

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

4.1 Checking vehicles

Drivers should visually check their vehicle at the beginning and end of their journey and whenever they leave or return to their vehicle to ensure that nothing has been concealed or tampered with. A Security top 10 list for Drivers (Annex A) supports this guidance.

4.2 Securing vehicles

Whenever vehicles are left unattended, for example at the start and end of a journey, during a comfort break or whilst parked securely as possible, drivers should ensure that all the doors and windows are closed, engine switched off and ignition keys are taken with them. For vehicles not requiring ignition keys, drivers should ensure that they secure the vehicle appropriately before leaving (Annex A).

4.3 What to do if a vehicle is taken

If your vehicle is stolen and you suspect it may be used in a terrorist attack call 999 and alert the call handler to the following information:

- Circumstances of the vehicle being stolen.
- Description of the vehicle including company name, registration details, aerial roof markings and any tracking software fitted in the vehicle.
- If you suspect that the vehicle has been stolen for a terrorist attack then make sure this is made clear to the call handler.

Drivers should also immediately alert their Transport Operators in their company

office who will have procedures in place for stolen vehicles.

4.4 Disposal of vehicles

Prior to disposal or sale to third parties, all vehicles should have their entire internal and external livery and other markings removed to avoid potential use by others for malicious purposes.

Annex A – Security Top 10 for Commercial Vehicle Drivers

1) Plan routes before beginning a journey and avoid using the same routes and stops for breaks routinely.

2) Avoid talking about loads or routes with other drivers or customers (including over radios and telephones) and do not post information about your route on social media.

3) Lock and secure your vehicle whenever you leave the cab and keep the keys with you at all times, including when unloading and loading, even if leaving the vehicle for a moment.

4) Carry out visual walk around checks when leaving and returning to the vehicle to make sure it has not been tampered with. Report any irregularity in loading, locking, sealing or documentation to your Transport Operator.

5) When doing walk around checks, think Security as well as Safety.

6) If you are forced to change your route, inform your Transport Operator immediately. Avoid stopping for scheduled breaks where possible.

7) If someone is acting suspiciously or something ‘doesn’t feel right’ either at the depot or on the road, report it to ACT, call 0800 789 321.

8) Do not allow unauthorised passengers into the cab.

9) Keep your phone fully charged and on you at all times.

10) Be mindful of your personal security when driving.

Annex B – Glossary of terms

ACT: Action Counters Terrorism, a national campaign by Counter Terrorism Policing to encourage the public to act on their instincts to help tackle the terrorist threat.

Cab: The cab is an enclosed space in a lorry where the driver is seated.

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

CTSA: A Police Counter Terrorism Security Advisor.

DVSA: Driver and Vehicle Standards Agency

DfT: The Department for Transport.

NaCTSO: the police National Counter Terrorism Security Office

NCTPHQ: National Counter Terrorism Police HQ

Operating centre: A base or depot for Commercial Vehicles

Suspicious Behaviour: Any observed behaviour that could indicate terrorism or terrorism-related crime

Transport Operator: Management working in the company offices and are responsible for managing the execution, direction, and coordination of all transportation matters within the organisation.

Annex C – Summary of Sources and Further Information

Section	Topic	Organisation	web link
Section 1: Introduction	CONTEST: The United Kingdom's Strategy for Countering Terrorism	HM Government	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
Section 2: Security Culture	Security Culture	CPNI	https://www.cpni.gov.uk/developing-security-culture
	ACT: Action Counters Terrorism	Counter Terrorism Policing	https://act.campaign.gov.uk/
	Embedding Security Behaviours: using the 5Es	CPNI	https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf
	Optimising People in Security	CPNI	https://www.cpni.gov.uk/optimising-people-security
	Insider Threat	CPNI	https://www.cpni.gov.uk/reducing-insider-risk
	Personnel Security	CPNI	https://www.cpni.gov.uk/personnel-and-people-security
	Pre-employment Screening	CPNI	https://www.cpni.gov.uk/pre-employment-screening
	British Standard for Security Screening Employees (BS7858)	BSI	https://shop.bsigroup.com/ProductDetail?pid=000000000030237324
	Pre-Employment Screening: Good Practise Guide	CPNI	https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf
	Crowded Places Guidance	NaCTSO	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf
Section 3: Site	Working with counter terrorism security advisers	NaCTSO	https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-

Security			counter-terrorism-security-advisers
	EC security guidance for the European commercial road freight transport sector	European Commission	https://publications.europa.eu/en/publication-detail/-/publication/677076fa-fc01-11e7-b8f5-01aa75ed71a1/language-en
	Control Access	CPNI	https://www.cpni.gov.uk/content/control-access
	Lone Working	HSE	http://www.hse.gov.uk/toolbox/workers/lone.htm
	Crowded Places Guidance	NaCTSO	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf
	CCTV Guidance	CPNI	https://www.cpni.gov.uk/cctv

Additional Sources

Topic	**Organisation**	**web link**
DfT Rental Vehicle Security Scheme (RVSS)	DfT	https://www.gov.uk/government/publications/apply-to-the-rental-vehicle-security-scheme
Dangerous Goods Security Training	DfT	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/318451/dangerous-goods-road-training.pdf
Bus and Coach Security Recommended Best Practice Third edition	DfT	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730644/bus-and-coach-security-recommended-best-practice.pdf
Fleet Operator Recognition Scheme	FORS	https://www.fors-online.org.uk/cms/
Professional driving of lorries, buses and coaches	DVSA	https://www.gov.uk/transport/professional-driving-of-lorries-buses-and-coaches