Department for Transport

Dangerous Goods Security Training

Guidance for the Design & Delivery of Security Awareness Training for the Carriage of Dangerous Goods by Rail & Road

v2.2
October 2011

Change control

Version	Changes	Approved by	Date
2	Revision and expansion of the 2005 guidance.	Guy Slaney	10/12/10
2.1	DfT contact details updated.	Guy Slaney	20/9/11
2.2	DfT contact details on driver advice sheet updated.	Guy Slaney	28/10/11

Notes

There is no security classification attached to this document.

This guidance relates to the security requirements for the carriage of dangerous goods by rail or road in Great Britain.

This document is formatted for 2-sided / duplex printing and some pages have been intentionally left blank.

Additional copies of this document can be obtained from the DfT website (search the Publications section for "dangerous goods security"). For any queries in relation to the content, please contact:

Dangerous Goods Industry Training
Department for Transport
2/34 Great Minster House
33 Horseferry Road
London
SW1P 4DR

DGSecurity@dft.gsi.gov.uk
020 7944 2881

www.dft.gov.uk

Contents

	Page
Guidance for Dangerous Goods Security Awareness Training	4
Recommended training content	6
Additional Guidance and Briefing Notes	9
Module 1 - The nature of security risks	*10*
Module 2 - Recognising security risks	*12*
Module 3 - Methods to address and reduce security risks	*14*
Module 4 - Actions to take in the event of a security breach	*18*
Annex A - Driver Advice Sheet	19

Guidance for Dangerous Goods Security Awareness Training

1. This guidance is provided to support the security training of all staff involved with the carriage of dangerous goods as set out in chapters 1.10 of RID and ADR, taking into account the provisions of chapters 1.3. For many companies, security measures will already be in place for commercial reasons and whilst this training focuses on the threat from terrorism, it shares the same basic principles of good security. Where relevant, it should be provided with a view to improving security in the round.
2. Nothing in this document should be seen as replacing or overriding either the current regulations relevant to the security of dangerous goods or any agreement(s) on security measures and operational practice that may have been reached with the DfT in specific circumstances. Any questions arising from this document, or on areas not covered by this document, should be directed to the DfT (see the contact details on page 2).

Course content and design

3. As this is a guidance document applicable to a wide range of operations, it is for the trainer to take this guidance and design a course programme appropriate to the needs of the target audience. This may include the production of more detailed training materials or the use of training aids (such as the training films available from the DfT - for further details see the DfT website). Much of the detailed course content will be drawn from local information and procedures relevant to the location(s) where the trainee will be working.
4. The detailed requirements for training should be established as part of the risk assessment process and will need to take into account the type(s) of dangerous goods being handled. Where High Consequence Dangerous Goods (HCDG) are handled, more detailed training may be appropriate. Any training delivered should cover only those topics that are relevant to the trainee.
5. For drivers carrying dangerous goods by road, the Driver Advice Sheet included at Annex A may also be relevant.
6. Employers should consider whether specific training is needed, or whether other existing training is sufficient to meet the requirements of RID and ADR (e.g. commercially-driven security training or Air Cargo Security training delivered in accordance with DfT requirements).

Target audience

7. RID and ADR require all persons engaged in the carriage of dangerous goods to consider the security requirements commensurate with their responsibilities. Security awareness training is mandatory appropriate to the person's responsibilities and duties and to the loads to be carried. This guidance is based around the following broad personnel groupings who will commonly be employed in the carriage of dangerous goods and require training:
   a. Administration personnel (e.g. consignor and consignee personnel responsible for paperwork; carrier personnel responsible for route planning; etc.).
   b. Operational personnel (e.g. loader; packer; filler; unloader; rail shunter; etc.).
   c. Security personnel (e.g. security guards; those responsible for access control; etc.).
   d. Drivers (rail), including any train crew.
   e. Drivers (road), including any vehicle crew.
8. Site / security managers should be able to demonstrate a comprehensive understanding of all the topics relevant to the operation(s) for which they are responsible. Senior staff (such as company directors and others whose appointments involve executive, operational or administrative responsibility for security) should also

be able to show an awareness of security appropriate to their responsibilities and the potential impacts on their business.

Trainers

9. Before they begin to deliver training, any trainer should at a minimum have a good understanding of the core principles of the security regime relating to the carriage of dangerous goods. Any trainer wishing to be kept up to date with information on the threat to transport security should contact the DfT (see the contact details on page 2).

Course frequency, duration and numbers

10. Initial training should be given to all personnel before they start to carry out any duties in relation to the carriage of dangerous goods. Under RID and ADR, personnel must be trained before assuming responsibilities and shall only perform functions for which required training has not yet been provided under the direct supervision of a trained person.
11. Course duration will vary according to the content covered, the number of staff being trained, the approach taken to the delivery of training, the nature of the assessed risk and the type of dangerous goods being carried. Where HCDG will be carried, longer and more detailed training will likely be appropriate.
12. The need to update staff on security issues should be reviewed every 2 years in light of the biennial revision of RID and ADR to ensure that the training that has been given remains current and correct. Refresher training should be provided at intervals of no more than 5 years but the use of a greater frequency should be considered as part of the risk assessment process.
13. The maximum number of trainees per course is left to the discretion of the trainer. However, every course should ensure that each trainee is given an appropriate amount of attention and time to understand the content and have their learning assessed.

Assessing learning

14. Each trainee should be able to demonstrate a satisfactory level of knowledge and understanding at the end of training. Learning could be assessed either as the training progresses or at the end of training. Any assessment of learning should be delivered in a manner suitable for the topic covered and the method of training used.

Training records

15. It is a requirement of RID and ADR that training records must be kept by the employer and made available to the employee upon request. These records should be kept for both initial and refresher training and should be retained at least until such time as the training for that individual has been updated. Records should at the minimum include:
    a. a unique identifier for the trainee (e.g. a name or staff number);
    b. details of the training delivered; and
    c. the date(s) on which the training was carried out.
16. It is recommended that the training record should also:
    a. include the duration of the training given;
    b. include the date on which duties relating to dangerous goods were first undertaken; and
    c. be retained at least for the duration of that individual's employment.

Quality assurance

17. The DfT may monitor the delivery of training where, in the case of inspection activity, problems have been identified. This will be carried out with the agreement of the employer / trainer.

Recommended training content

This section sets out the common aims, objectives and competencies that should be considered in the design of security training. The Training guidance matrix is provided as an indication of the key objectives that will normally be relevant for the training of the different groups of personnel commonly found in the industry but it is not exhaustive and may not always be applicable.

Further guidance and briefing notes to support the Training guidance matrix are provided in the Additional Guidance and Briefing Notes section starting on page 9.

Course aims

1. To provide all staff involved in the carriage of dangerous goods with a working understanding of the relevant security risk(s).
2. To ensure that all staff involved in the carriage of dangerous goods understand their role and responsibilities in providing and maintaining effective security.

Course objectives

1. For trainees to understand the threat facing the carriage of dangerous goods and how it is assessed.
2. For trainees to understand the vulnerabilities surrounding the carriage of dangerous goods.
3. For trainees to understand their role in implementing and maintaining effective security.

Personnel Competencies

Once trained, personnel should be able to demonstrate the following competencies:

Performance - the trainee should be able to (as relevant to their role):

a) Identify sources of threat to the security of dangerous goods.
b) Identify vulnerabilities and carry out the appropriate security-related activities to counter these.
c) Respond to potential risks in a timely manner.
d) Take appropriate action when a security breach is identified.

Knowledge - the trainee should know and understand (as relevant to their role):

a) Who poses a threat to the security of dangerous goods and why.
b) How the threat relates to vulnerability and risk.
c) The key areas of vulnerability relevant to their role.
d) The standard practices and procedures that should be adopted to reduce vulnerabilities and any additional specific security duties that the trainee is required to undertake.
e) The appropriate steps to take when a potential security risk is identified.
f) The action to be taken when a security breach is identified.
g) The role of government agencies in monitoring compliance.

It is recommended that some form of assessment of the relevant competencies is made at the end of the training e.g. by a short Q&A, discussion or test.

Training guidance matrix

Objectives	Personnel groupings					
	Admin. personnel	Operational personnel	Security personnel	Drivers & crew (rail)	Drivers & crew (road)	Managers[b]
Module 1 - The nature of security risks						
1. For the trainee to understand the meaning of the word 'threat' in a security context and how it relates to risk.	X	X	X	X	X	X[b]
2. For the trainee to understand the types of people or organisations who may pose a threat to the carriage of dangerous goods, and why.	X	X	X	X	X	X[b]
3. For the trainee to understand the types of threat to the security of dangerous goods.	X	X	X	X	X	X[b]
Module 2 - Recognising security risks						
1. For the trainee to understand and be able to recognise potential vulnerabilities, both common and uncommon.	X	X	X	X	X	X[b]
2. For the trainee to understand the key areas of vulnerability for sites.	X	X	X			X[b]
3. For the trainee to understand the key areas of vulnerability whilst in transit.				X	X	X[b]
Module 3 - Methods to address and reduce security risks						
1. For the trainee to understand how the assessed risk affects the security measures applied.	X	X	X	X	X	X[b]
2. For the trainee to understand the need to protect information.	X	X	X	X	X	X[b]
3. For the trainee to understand what should be done to reduce the vulnerability of a site.	X	X	X	[a]	[a]	X[b]
4. For the trainee to understand the security measures which should be applied when transporting dangerous goods by rail.				X		X[b]
5. For the trainee to understand the security measures which should be applied when transporting dangerous goods by road.					X	X[b]
6. For the trainee to understand the role of government agencies in monitoring compliance and ensuring appropriate security measures are being applied.	X	X	X	X	X	X[b]
7. Additionally, where a security plan exists: for the trainee to understand the relevant details of the security plan.	X	X	X	X	X	X[b]
Module 4 - Actions to take in the event of a security breach						
1. For the trainee to understand what procedures should be followed in the case of a security breach.	X	X	X	X	X	X[b]

[a] Some elements of this objective may also be relevant to the training of drivers and crew.

[b] Managers should receive appropriate training which covers all the topics relevant to the operation(s) for which they are responsible.

Additional Guidance and Briefing Notes

Module 1 - The nature of security risks

Trainer notes

This module is intended primarily to provide suitable context and background information to trainees. The DfT use a risk management methodology based on the principle that 'risk' is a product of 'threat x vulnerability'. This module focuses on 'threat' with 'vulnerability' covered in modules 2 and 3.

Background information on the terrorist threat to the UK can be found on the Security Service website (www.mi5.gov.uk). In addition, regular updates on the terrorist threat will also be provided to those trainers who choose to notify their interest to the DfT.

Note that the appropriate level of detail to be covered in this module will vary depending on the type of dangerous goods being handled. Where HCDG are being handled, more detailed training may be appropriate.

Refresher training

Refresher training for this module should include:

1. Revisiting the relevant points for each objective.
2. Any changes to the threat and any incidents which have occurred since the last episode of training.

Aim and objectives

Aim

- To explain the nature of the threat to dangerous goods.

Objectives

1) For the trainee to understand the meaning of the word 'threat' in a security context and how it relates to risk.

2) For the trainee to understand the types of people or organisations who may pose a threat to the carriage of dangerous goods, and why.

3) For the trainee to understand the types of threat to the security of dangerous goods.

By the end of training, the trainee should be able to (as relevant to their role)

- Identify the types of people or organisation who may pose a threat to the security of dangerous goods and why.
- Explain the types of threat to the security of dangerous goods.

Briefing notes

Objective 1

- Risk is assessed using the principle that: Threat x Vulnerability = Risk.
  - **Threat** is a measure of the likelihood or probability of an attack against a particular target. It can be defined as 'the probability of an attack being attempted against a target within a specified time frame'. Threat is owned by the attacker.
  - **Vulnerability** is a measure of the features of a potential target which can be exploited by an attacker. It can be defined as 'those characteristics of a target which could be exploited in an attack'. Vulnerability is owned by us.

  - **Risk** is a measure of the probability that an attack will be attempted which will succeed in exploiting the target's vulnerabilities.
- Many things are taken into account when assessing the threat, including: current intelligence (e.g. terrorist motivation and intent); the characteristics and objectives of potential attackers (e.g. the known means / capabilities of terrorist groups); and the consequences / impact of an attack (whether successful or not – consequences can be defined as 'the human, economic, political and / or reputational impact of an attack').
- At the national level, the security services assess the threats from international terrorism and domestic extremism. These threat assessments are passed to the DfT who are responsible for deciding on the appropriate response to the assessed threat (i.e. the minimum measures that the industry must apply). When considering the appropriate response, the DfT use risk management methodology and where possible consult industry representatives.
- At the local level the risk assessment process is used to review threat and vulnerability, resulting in appropriate security measures that aim to minimise risk and prevent unlawful interference with the carriage of dangerous goods.

Objective 2

- Common sources of threat may include: terrorists (both international and domestic); criminals; the mentally ill; and protesters (e.g. environmental / animal rights). The ‘insider’ threat (i.e. a person employed at the site) should also be considered and this could include disaffected staff, recently dismissed staff seeking 'revenge' or staff manipulated through coercion or skilled influencing techniques to seek to cause harm. People can unwittingly become an insider, believing that they are merely ‘doing a favour’ for a friend or relative or satisfying intelligent curiosity. Other factors such as politics or disaffection, can also motivate a person to become an insider after several years in post.
- Dangerous goods are under threat as some have the potential to be used as a weapon to create a 'spectacular' (e.g. by using dangerous goods as part of an attack against a high profile / commercially valuable / prestigious target). A 'spectacular' may be sought in order to force a government reaction and generate substantial media coverage. The motives of individuals and groups seeking to cause a spectacular can include: gaining publicity for their cause; gaining the release of prisoners; changing government / international policy; frightening the public and disrupting normal life; obtaining money by threat / blackmail; undermining and discrediting authorities who oppose their cause.

Objective 3

- Common types of threat may include: hijacking of carried loads; sabotage of vehicles carrying dangerous goods; theft of a loaded vehicle from a site; the purchase of material without proper checks of the buyer being completed.
- Some loads that are ready or being prepared for transport may be at greater risk than others where they are relatively easy to transport once stolen.

Module 2 - Recognising security risks

Trainer notes

Training under this module should focus on two points: that everyone has a part to play in ensuring effective security is maintained; and the vulnerabilities that are relevant to where the trainee will be working. It may prove most effective to combine this module with Module 3, setting out the vulnerabilities together with the appropriate response.

Note that the appropriate level of detail to be covered in this module will vary depending on the type of dangerous goods being handled. Where HCDG are being handled, more detailed training may be appropriate.

Refresher training

Refresher training for this module should include:

1. Revisiting the relevant points for each objective.
2. Any changes to the known vulnerabilities and any new vulnerabilities identified since the last episode of training.

Aim and objectives

Aim

- To explain the vulnerabilities to the security of dangerous goods.

Objectives

1) For the trainee to understand and be able to recognise potential vulnerabilities, both common and uncommon.

2) For the trainee to understand the key areas of vulnerability for sites.

3) For the trainee to understand the key areas of vulnerability whilst in transit.

By the end of training, the trainee should be able to (as relevant to their role)

- Identify the areas of vulnerability relevant to their role and duties.

Briefing notes

Objective 1

- Details of vulnerabilities should be drawn from the relevant risk assessment(s).
- Examples of common vulnerabilities that all personnel should be aware of may include: no access control measures being applied to sensitive areas (e.g. pumping stations, administration facilities); loaded vehicles left unlocked with the keys in the ignition / cab; vehicle keys left insecure / accessible to people not authorised for access to a vehicle; areas used to store dangerous goods temporarily not being adequately secured / monitored; delivery / scheduling details (paper or electronic) not being adequately secured; a lack of proper checks of people seeking access to HCDG.
- Examples of uncommon vulnerabilities may include hostile reconnaissance and the insider threat.
    - Reconnaissance is considered to be an integral part of operational activity for terrorists and evidence suggests that hostile reconnaissance activity will be undertaken prior to any attack. Hostile reconnaissance may include: unusual questions about the type of security in place at a site; vehicles parked in suspicious circumstances around a site

perimeter; persons filming or taking photographs of a site for no apparent reason; individuals loitering outside a site perimeter for an extended period of time for no apparent reason and acting in a suspicious manner (e.g. taking notes, watching people enter or exit etc.); individuals bringing (or attempting to bring) unusual packages onto a site; suspicious behaviour by an individual attempting to enter a site (e.g. subject is nervous, perspiring, wearing inappropriate clothing, etc.); unusual occurrences (e.g. members of the public found in areas normally restricted to staff only) particularly in parts of the site allowing access to HCDG.

- The risk posed by the insider threat, including contractors and anyone else with access to physical or information assets, exploiting their legitimate access for unauthorised purposes is managed through personnel security measures. Personnel security is not just about pre-employment checks and ongoing measures should be considered as appropriate (e.g. being alert for changes in behaviour of staff, enabling staff to express any concerns about colleagues in confidence, regular reviews of access & clearances, etc.). An employee or contractor can become a security concern at any time and concerns may be raised by anyone who has come into contact with the individual. All personnel are encouraged to remain vigilant for potential signs that an individual may now present a risk. Some potential warning signs are: drug or alcohol misuse; support for extremist views (particularly when violence is advocated); a sudden change in religious, political or social affiliation that has an adverse impact on performance or attitude to security; major, unexplained changes in lifestyle; a sudden loss of interest in work, or very negative reaction to career changes or disappointments; signs of stress such as excessively emotional behaviour; sudden changes in working patterns (working alone, unusual hours or reluctance to take leave); being clearly unhappy, having few friends and appearing to be alienated from colleagues.
- To be fully effective, personnel and physical security measures mutually reinforce each other – a failure to properly apply one measure can weaken others (e.g. a site with a physical barrier also needs reliable security staff to help control access; and security staff also need a reliable physical barrier to help control access).

Objective 2

- Details of vulnerabilities should be drawn from the relevant risk assessment(s).
- Potential site vulnerabilities may include: access points (both pedestrian and vehicle); vehicles being allowed on-site; site perimeter and buildings; people.
- The vulnerability of information should also be considered, such as: details of the storage and transport of dangerous goods; site procedures for access control and security.

Objective 3

- Details of vulnerabilities should be drawn from the relevant risk assessment(s).
- Potential vulnerabilities whilst in transit may include: carrying unauthorised passengers; parking the vehicle in an insecure location; not activating the immobiliser / anti-theft device when leaving the vehicle; traffic stops being applied by criminals to gain access to the vehicle / load.

Module 3 - Methods to address and reduce security risks

Trainer notes

The focus of this module should be on the activities and tasks that the trainee can undertake to reduce vulnerability and improve security. Special attention should be paid to instilling a security culture in all trainees. This module should form the bulk of any assessment of learning.

Objective 3 is intended for personnel working at sites but some elements of this may also be useful to drivers and crew.

Note that the appropriate level of detail to be covered in this module will vary depending on the type of dangerous goods being handled. Where HCDG are being handled, more detailed training may be appropriate.

Refresher training

Refresher training for this module should include:

1. Revisiting the relevant points for each objective.
2. Any changes to the security measures and any new security measures implemented since the last episode of training.

Aim and objectives

Aim

- To explain the trainee's role in reducing vulnerability.

Objectives

1) For the trainee to understand how the assessed risk affects the security measures applied.

2) For the trainee to understand the need to protect information.

3) For the trainee to understand what should be done to reduce the vulnerability of a site.

4) For the trainee to understand the security measures which should be applied when transporting dangerous goods by rail.

5) For the trainee to understand the security measures which should be applied when transporting dangerous goods by road.

6) For the trainee to understand the role of government agencies in monitoring compliance and ensuring appropriate security measures are being applied.

Additionally, where a security plan exists:

7) For the trainee to understand the relevant details of the security plan.

By the end of training, the trainee should be able to (as relevant to their role)

- Explain when and how to apply the security measures relevant to their role.
- Where one exists, explain any responsibilities under the security plan.

Briefing notes

Objective 1

- The security measures and procedures implemented locally exist as a result of the risk assessment process. Security measures will commonly exist in two forms: mitigating measures (also known as countermeasures) which form part of the standard routine; and contingency plans prepared to respond to specific incidents, should they occur.

Objective 2

- Everyone who works in the carriage of dangerous goods plays a vital part in the protection from those who wish to do us harm. The integrity, discretion, and trustworthiness on the part of those working in the sector are an important part of the effectiveness of security.
- Hostile reconnaissance may include people involved with the carriage of dangerous goods being approached with questions about the security measures that are applied. Such situations should be treated with caution and generally, when outside the workplace, personnel should not discuss with anyone the details of security procedures, types of dangerous goods being handled or stored, or possible routes used for transit.

Objective 3

- The overall security measures applied locally should be explained. This should cover both the general measures that all personnel should apply and the role(s) of any personnel with specific security duties (e.g. access control).
  - Common security-related activities that all personnel on a site should undertake as part of their normal duties could include: displaying access passes visibly at all times; checking the access passes of others and challenging people not displaying a suitable pass; identifying security breaches and reporting these to the appropriate person (e.g. a supervisor or the site / security manager).
  - Specific duties that the trainee is required to undertake should be explained in the context of how these will reduce the vulnerability of the site. These could include: carrying out suitable checks on staff before they are employed; controlling access to critical areas; keeping keys for vehicles and delivery paperwork secured until the driver is ready to take the vehicle; checking the credentials of people collecting dangerous goods; storing information securely and only providing it to those people who are both authorised to have it and have a valid reason for access to it.
- Any specific reporting procedures (e.g. if hostile reconnaissance is suspected) should be explained.

Objective 4

- Drivers and any train crew must always carry a suitable form of photographic ID document (this is a statutory requirement) so that their identity can be verified at collection and delivery sites.
- Any relevant local / company procedures relating to the carriage of dangerous goods by rail should be explained. This may include: any procedures to undertake before taking control of a train; things to consider whilst in transit; and any procedures to follow when arriving at the point of delivery.

Objective 5

- Drivers and any vehicle crew must always carry a suitable form of photographic ID document (this is a statutory requirement) so that their identity can be verified at collection and delivery sites.
- Things to consider when planning routes:
  - Wherever possible, delivery routes should be pre-planned with a copy of the route held at base and the details of the route restricted to those who need to know. Where a route includes stops, secure parking should be used where possible.

- Things to consider before taking control of a vehicle:
  - A security inspection of the vehicle should be carried out (this may be done as part of the safety inspection) looking for signs of tampering or other irregularities, such as: damage to locking and other mechanisms to secure the load; damage to the fabric of the vehicle which may impair the effectiveness of seals (e.g. cuts or tears in curtains).
  - If appropriate, apply / check security seals to the load compartment.
  - The delivery paperwork should also be checked for signs of tampering, amendments, or other irregularities such as sudden or last minute changes to delivery instructions.
  - Drivers should understand how to operate any security equipment installed on the vehicle(s) that they will be using (e.g. immobilisers, locking systems, vehicle trackers etc.).
  - The appropriate procedures for reporting any concerns over tampering, irregularities or security equipment that is not working correctly should be explained.
- Things to consider when in transit:
  - It is illegal to carry unauthorised persons when transporting dangerous goods.
  - If a pre-planned route has to be changed whilst in transit, it may be appropriate for the driver to contact base and agree a revised route before proceeding.
  - Other than pre-planned stops, reasonable efforts should be made to not stop whilst in transit. However, if stopping is unavoidable the vehicle should be parked so that it can be kept under observation by the driver at all times and the parking location used should be sufficiently secure and fit for purpose - insecure or 'casual' parking spots and standard patterns (e.g. always stopping at the same place to pick up supplies) should be avoided.
  - When leaving the vehicle, the cab should be secured and any immobiliser / anti-theft devices that may be fitted should be enabled. When returning to the vehicle after a stop, a cursory security inspection should be carried out to ensure that the vehicle has not been tampered with or otherwise compromised whilst parked.
  - Caution should be used when asking for directions or advice about suitable off-road parking facilities.
  - Where the journey includes an overnight stop, pre-planned, secure overnight parking facilities that are suitable for the dangerous goods being carried should be used and all doors should be locked whilst sleeping in the cab.
  - Keys should be kept secure at all times and never be left in a hiding place for a relief driver.
  - Trailers or containers should only be left in pre-agreed parking areas with approved security devices fitted / enabled.
  - The appropriate procedures to be followed in case of an emergency should be explained.
  - Where HCDG are carried, the driver may need to be issued with a dangerous load card. This is to be used only when the vehicle is stopped by the police or VOSA (Vehicle and Operator Services Agency) and the driver has concerns about the validity of the officer(s). In these circumstances, the driver should not leave the vehicle but display the dangerous load card clearly to the officer(s) and not open the vehicle until the identity of the officer(s) has been verified.
- Things to consider when arriving at the point of delivery:
  - Ensure that the delivery point matches the delivery paperwork and be wary of deception.
  - Where possible, the cab should be secured and any immobiliser / anti-theft device activated whilst unloading the vehicle.

Objective 6

- The DfT is the regulator for transport security in the UK (excluding rail and dangerous goods in Northern Ireland). This role includes responsibility for setting government policy and the minimum standards for security as well as ensuring that these policies and standards are implemented through compliance monitoring. Compliance monitoring is primarily achieved through inspections: the security of dangerous goods transported by rail, along with any related sites, is inspected by DfT Transport Security Inspectors; the security of dangerous goods transported by road, along with any related sites, is inspected by VOSA traffic examiners.

Additionally, where a security plan exists:

Objective 7

- The details of the security plan that are relevant to the trainee should be explained including any responsibilities the trainee has as part of the normal routine. When discussing the security plan, the following points should also be covered:
  - Any plan is only as good as the people responsible for implementing it and security plans should be tested regularly to ensure that everyone affected understands their role. Testing the plan also checks whether the plan itself is sufficiently fit for purpose and may result in the plan being updated.
  - The security plan contains sensitive information and access to it should be limited to only those persons who are authorised to have access in relation to their duties. The contents of the plan should not be discussed with anyone outside of the organisation / site to which the plan relates. Any discussion of the plan with people employed by the organisation / at the site to which the plan relates should be limited to that which is necessary to understand the requirements of the plan.

Module 4 - Actions to take in the event of a security breach

Trainer notes

This module focuses on what needs to be done when a security breach has occurred but it should also be used to reinforce the message that the prevention of a breach is preferable to reacting to one.

Note that the appropriate level of detail to be covered in this module will vary depending on the type of dangerous goods being handled. Where HCDG are being handled, more detailed training may be appropriate.

Refresher training

Refresher training for this module should include:

1. Revisiting the relevant points the objective.
2. A summary of any security breaches that have occurred since the last episode of training with an emphasis on the lessons learnt.

Aim and objective

Aim

- To explain the appropriate response to security breaches.

Objective

1) For the trainee to understand what procedures should be followed in the case of a security breach.

By the end of training, the trainee should be able to (as relevant to their role)

- Explain what constitutes a 'security breach' and the steps to be taken when one is detected.

Briefing notes

Objective 1

- A security breach can be defined as 'an activity or occurrence which indicates that the security of dangerous goods has been compromised'. Security breaches may include: a vehicle being tampered with; a fence being cut or otherwise broken through; an unauthorised person in a storage site; theft of a vehicle (either from a site or whilst the vehicle is in transit); theft of the paperwork relating to a delivery.
- The standard procedures to follow when a security breach (either suspected or actual) is identified should be explained. This may include duties under evacuation procedures or who to notify about the breach.
- Any specific responsibilities that the trainee may have in the contingency plan(s) that relate to security breaches should be explained.
- If relevant, any specific procedures to be followed as set out in the security plan should also be covered here.

Annex A - Driver Advice Sheet

Introduction

More than 3,000 HGVs are stolen in the UK every year and only about 12% are ever recovered. Half of all stolen trucks are stolen from their own premises.

Your truck is your livelihood. The tips in this fact sheet will help you stop truck thieves. Please take the time to read this leaflet and discuss any questions you may have with your employer. Keep it safe in your cab for future reference.

If you witness suspicious or criminal behaviour, call the police immediately by dialling 999. Always let your employer know what is happening.

If you suspect terrorist involvement then also call the Anti Terrorist Hotline on 0800 789 321.

Be Secure

When you leave your vehicle, always lock it and always take your keys with you. Never leave them in the cab.

Always make sure your cab and, where appropriate, the load compartment are secure.

- When loading or unloading, lock the cab.
- When driving, where appropriate, lock the load compartment.
- Check that all security devices are working.

If you keep the lorry keys when you are not at work:

- make sure they cannot be identified – don't leave anything on the key ring that tells who they belong to or what vehicle they fit;
- never leave them where strangers can see them; and
- always keep them somewhere safe.

If you keep your keys at the operating centre:

- make sure they are in a lockable place out of sight of strangers; and
- never use a 'hiding place', for example, inside the front bumper.

The theft of vehicle keys is on the increase, so be warned!

Park Safely

- Whenever possible decide where you are to park overnight before starting your journey.
- Park your vehicle within sight and where you can return to it quickly for short breaks.
- When returning, check all round for signs of interference, including any load security seals.
- When returning to the UK from Europe, be particularly alert for signs of illegal immigrants and be aware of any special instructions at ports and the Eurotunnel.

Plan Ahead

- Plan your route beforehand. That way you will not have to stop to ask directions. If you know exactly where you are going, no-one can mislead you with wrong directions.
- Be unpredictable in your daily work pattern.

Be Aware

- Avoid talking about loads or routes with other drivers or customers (including over radios or phones).
- Be cautious if you are forced to stop, for example, at the scene of an accident or an emergency, or at police stops.

If you are carrying a dangerous load card:

- keep it safe; and
- if you are stopped by the police or VOSA and are suspicious about the validity of the officer, follow the instructions on the reverse of the card.

During security alerts, follow the advice given to you by local police. At these times only, make sure:

- someone competent stays with your lorry; and
- if you are alone, you leave a clearly displayed note explaining how you can be contacted.

Everyday Security

- Avoid regular routes or stops for newspapers, cigarettes or meals – a recognisable pattern makes you an easier target for thieves.
- Never give lifts; it is illegal to carry unauthorised persons when transporting dangerous goods.
- Make sure you understand and use the vehicle's security equipment and check it's working properly.
- Never leave keys in or on your truck.
- If your truck or trailer has a roof marking and you are the victim of a crime, make sure you tell the police.

Documents

When you collect a load:

- check the load matches the collection note;
- make sure it is clear where you are delivering to and who will receive the goods;
- get a contact number if you can; and
- record the load seal number, if appropriate.

When you deliver:

- check the load seal is intact and the number is the same as on the delivery note;
- check that quantities and weights match the collection and delivery notes;
- make sure you are delivering to the right place (check collection and delivery against the notes);
- if the delivery instructions are changed, get written confirmation of the changes from senior staff at the delivery address or from your employer; and
- make sure that there is a clear signature and printed name on the POD (proof of delivery note).

Protect Your Own Belongings

- Hide personal property from view.

Company Security

Your company security instructions and procedures are designed to protect your vehicle and its load. Follow them at all times.

If you fail to follow them, your employer could take disciplinary proceedings against you, the driver.

Remember, if you lose your truck, you could lose your job.

If you see anything suspicious, report it to the police by dialling 999, and to your employer.

Call Crimestoppers on 0800 555 111 if you have any information about truck crime or any other crime. Your call is free. You do not have to give your name. You may receive a reward.

Published by the Department for Transport.

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