CONSOLIDATED GUIDANCE FOR THE SECURITY OF DANGEROUS GOODS BY ROAD

This guidance outlines ways in which the Voluntary Code of Practice for the Security of Dangerous Goods by Road could be met. It is not intended to be a prescriptive document and organisations are free to use different ways of complying with the Code.

Published by the Department for Transport.

Department for Transport
Great Minster House
76 Marsham Street
London SW1P 4DR
Telephone 020 7944 8300
Internet service wwww.dft.gov.uk

Revision 1
March 2004

CONTENTS PAGE

Introduction

Any incident involving dangerous goods is potentially very serious, especially if it involves high consequence dangerous goods - see Annex 3.

That is why the Government is trying to make dangerous goods less vulnerable while they are being transported. The Government wants to introduce a number of security measures by way of a voluntary code of practice. We want to do this before any amendments to the United Nations Model Regulations come into force in the UK.

The Department for Transport has set up an advisory group for the security of transport of dangerous goods by road, to develop the voluntary code of practice and the guidance that goes with it. The group consists of representatives from:

- various Government departments, including the Department for Transport;
- police and law enforcement agencies; and
- industry associations.

The Department has produced these guidance notes to help organisations deliver the voluntary measures in the security code of practice. We do not intend this to be a prescriptive document.

The guidance applies to all classes of dangerous goods transported by road. But it separates those measures that are appropriate to the transport of all dangerous goods from those additional measures that are appropriate to the transport of high consequence dangerous goods - see Annex 3.

Each organisation should assess its own vulnerabilities. This guidance will help with that process. The measures outlined should be viewed as ways in which the code of practice could be met. Organisations should determine whether, and how far, to apply those measures.

These recommendations are part of wider Government efforts to:

- improve the resilience of the UK, and

- help industries to protect themselves against a range of threats including accidents, deliberate sabotage and acts of terrorism.

It is vital to build security into everything we do. It is important for businesses and organisations to take responsibility for helping to tackle the problem, and to encourage a culture of security awareness. Everyone whose work involves the transport of dangerous goods should be in the daily habit of taking security measures.

1. People – introduction

Workforce security plays an important part in any integrated approach to protecting a business from threats, including terrorism. Workforce security can raise difficult and sensitive issues for employers and managers, as well as for individual employees. Any measures need to be proportionate to the perceived risks.

Many external threats to a business or organisation depend to some degree upon the co-operation of an 'insider'. This could be a permanent or temporary employee. It could be contract or agency staff, such as a driver, cleaner, caterer or security guard, who is given access to business premises. 'Insiders' may be recruited from among existing staff, or they may be new staff deliberately infiltrated into the business.

The key question in relation to workforce security is:

> Are the people in the workplace who they say they are and should they be there?

Many factors will affect the level of risk, including:

- site location;
- nature of operations;
- number of people employed;
- number of contractors; and
- vehicle access to the site.

A review and risk assessment of workforce security systems should be part of a risk management approach to security.

Any person engaged in the transport of dangerous goods should consider security requirements according to their responsibilities.

Businesses and organisations should check the credentials of individual employees and contractors or agency staff. You can do this directly when you draw up an employee's contract of employment, or indirectly with contractors as part of the overall contract.

1.1 Recruitment

1.1.1 Appropriate persons

Reliable and responsible staff are central to making sure that other security measures work effectively. You should get documentary evidence of the background, experience and character of anyone you are thinking of recruiting.

Organisations should ensure all employees who are involved with the transport of dangerous goods are suitable for the task and that they hold verifiable:

- licences, certificates and operating documents where applicable; and

- permission to work in the UK where necessary.

Warn applicants that giving false information, or failing to disclose material information, would be grounds for a refusal to interview or, if employed, dismissal.

Companies should also regularly verify any licences, certificates and operating documents that staff may need to do their job.

1.1.2 Employment checks

You should check the employment record of everyone involved in the transport of dangerous goods. You should get documentary evidence of background, experience and character for all potential employees. Insist on original documents to check identity and qualifications.

Ask the candidate for the following information:

- full name;
- address;
- date of birth;
- National Insurance or other unique personal identifying number where appropriate;
- details of any past criminal convictions (where this is allowed by law); and
- full details of references (where applicable).

You should get a continuous record of the applicant's education and employment history. This may not always be easy, but in general ask for information covering the preceding 10 years, and as an absolute minimum covering the previous five years.

- If possible speak directly with the previous employer(s) and discuss the applicant' s work record and character.
- When checking references by phone, get the number you need from a telephone directory or enquiries service. Any number supplied by an applicant could be that of an accomplice.
- Do not accept open references such as 'to whom it may concern'.
- You should get confirmation in writing from employers, educational authorities, and so on.
- Insist on seeing the applicant's original birth certificate, not a photocopy. Obtain a recent photograph of the applicant and get him/her to sign it in the presence of a company representative (see also section 2.2.2).
- Keep a progress sheet to record all the actions you take.

You should check identities by asking to see a passport, an official photo ID (such as the new-style driving licence), utility bills sent to the applicant's address and so on. Where appropriate, you should also verify proof of right to live and work in the UK.

Check driving licences thoroughly:

- Compare the stated date of birth against the birth certificate. An ordinary licence will expire the day before the holder's 70th birthday. A driving licence contains important personal information about the holder. Ask the applicant for his or her date of birth. Only give them one opportunity to get it right.

- Examine the licence closely for signs of alteration, discolouration or erasure. Make sure that the pink and green background is intact. Be suspicious of stained or damaged licences. Check for endorsements. Photocopy the licence and keep the copy on file.

- Duplicate licences usually have "duplicate" printed on them. Most are issued for legitimate reasons, but be aware that disqualified drivers have been known to use duplicates to get driving work.

You can gather much of this information as part of a well-structured interview.

1.1.3 Contractors

Businesses use contractors or agencies to provide a growing range of services. Examples include drivers and warehouse or depot staff.

But contractors may create new vulnerabilities and expose businesses to a greater 'insider' threat than they would face if relying on directly recruited staff. Some contractors or agencies may be less rigorous in their selection procedures than those who use their services would be.

Contractors involved in the transport of dangerous goods should undergo the same pre-employment screening process as new employees. Responsibility for implementing these checks will rest with the supplying company. The user company should ask them to demonstrate, from their records, that they have carried out these checks. If they fail to do so, the employing company should review its working relationship with the contractor. The supplying company should demonstrate compliance with BS 7858 (Code of Practice for screening of personnel).

User companies may sometimes employ large numbers of contractors on a specific project, at a separate site - for example construction of a new process. In these circumstances, user companies may consider reducing their screening procedures, provided that they can prevent the contractors from gaining access to the operating site.

The user company may have to assume responsibility for carrying out the checks on behalf of self-employed contractors.

Organisations should consider additional checks or screening of contractors or sub-contractors employed in key positions, such as security guards at site access points.

It is worth establishing whether the contractor or agency is part of a recognised professional organisation which accredits standards in that industry.

Another good practice is to ensure that you have procedures to confirm that a person sent by a contractor or agency is indeed the individual who turns up.

You might achieve this by the following procedures:

- Require the contractor or agency to provide in advance a photo of the individual, authenticated by them. You can compare this with the person who turns up at your premises before you let them in.
- Require the contractor or agency to provide their own photo ID, which you can check on each entry.
- If you provide your own permanent staff with a photo ID, extend this to contract staff. Ideally you should retain these passes between visits. On each visit, compare the contractor or agency staff member with their photograph before handing them the pass.
- Have an agreed substitution procedure for contract staff who are temporarily absent. This could include setting out what is acceptable in terms of a temporary replacement, and considering whether to restrict their duties or access.

1.1.4 Existing employees - high consequence dangerous goods

There are obvious sensitivities when it comes to your own staff. In the vast majority of cases, your employees will have exemplary employment records. And apart from the issue of sensitivity, both employee and employer will be bound by a contract of employment.

You will need to check existing employees who work on sensitive sites in order to ensure the integrity of the overall system.

You should ensure that you have similar information on file for existing staff as for new employees – see also section 1.1.2 (Employment checks).

In some cases this information may not have been gained at the time the employee had taken up employment, may have been discarded or is simply out of date. You need to check and update it regularly.

If this process provokes any security-related questions you should raise these with the individual concerned in the first instance. At this stage the employee should have the right of representation.

It is good practice to draw up a security policy statement. This should set down general principles for the secure operation of vehicles and the serious view taken of dishonesty, irresponsibility or negligence. You might include this in the company driver's handbook.

1.2 Training

1.2.1 Training and awareness

Companies should provide security awareness training for everyone involved in the carriage of high consequence dangerous goods. You should periodically supplement initial training with retraining.

The training should deal with:

- the nature of security risks;
- recognising security risks;
- how to minimise security risks; and
- what to do in the event of a security breach.

The training should also include awareness of security plans (if appropriate). This should be at a level appropriate to the responsibilities of individuals and their part in implementing security plans.

The employer should record all security training and make the records available to the employee if asked.

1.2.2 Training and awareness – high consequence dangerous goods

Brief drivers on what to do in the event of hijack or criminal attack. Emphasise that they must not put themselves at risk in an attempt to protect the vehicle and load.

1.2.3. Driver training – high consequence dangerous goods

The training programme for drivers who transport high consequence dangerous goods should include the following elements.

- A drivers' handbook, which covers security measures and procedures for the vehicle, load and company premises. The security section of the handbook should specifically prohibit unauthorised person(s) in the cab and include guidance to drivers on theft of their load by deception.

Instruction in the right security habits. Drivers should see security as a normal, daily routine in the workplace.

- Instruction in the driver's security role, including how to use the security equipment fitted to the vehicle and at the company's premises, where appropriate.
- Hijack awareness/avoidance.

A video to help train drivers has been produced by DfT TRANSEC and can be obtained on application. Further details can be found on the TRANSEC website.

2. Procedures - introduction

This section highlights effective measures which organisations involved with the transport of dangerous goods can take to improve security procedures. Incidents sometimes occur because of a failure to recognise risks and adopt basic security measures.

Operators should continually refine their security procedures.

2.1 Companies

2.1.1 Employees and contractors - monitoring behaviour

Employers can try to identify potential risks by encouraging both managers and staff to be alert to changes in employees' behaviour and attitudes. These might suggest potential conflicts of interest or disaffection that could undermine trust in them.

This can be controversial, however. No employer or co-worker wants to be accused of prejudice, of over-reacting to legitimately held opinions, or of being a 'sneak'.

If you do have concerns, act sensitively. It is best to be as open as possible with the individual concerned and explore the issue in a constructive, non-threatening manner.

Employees must be given the confidence to report things and must know that their employer will take their reports seriously and treat them confidentially. Any action resulting from such reports must be in accordance with employment law, other legislation such as the Human Rights Act and the Data Protection Act, and best practice.

It is easier to monitor behavioural changes in your permanent staff than it is with contract staff, who may not be as well known to you. Employers should consider:

- providing permanent supervision, either throughout the period when the contract/agency staff are on the premises, or when they have access to particularly sensitive or business critical areas;

- nominating a permanent employee to be responsible for the contract staff as individuals, not just for overseeing delivery of the contract. This member of staff could then pick up on any concerns about potential conflicts of loyalties and the like, both with the individual and with the contractor/agency manager responsible for oversight of the contract.

2.1.2 Management routines and secure working practices

There are a number of routines that you can adopt to improve security.

Managers should:

- constantly review operational procedures;

- consider possible risks and always bear security measures in mind;

- keep documentation about the load in a secure place. Criminals could use consignment documentation to show they have title to the goods;

- keep all vehicle/premises keys in a secure place. Managers should develop secure practices for controlling keys to vehicles and premises - see section 3.1.14 (Key control);

- where possible, vary routes and drivers to avoid regular patterns developing;

- consider joining the Metropolitan Police TruckPol scheme - see section 2.2.5 (Reporting Security Incidents); and

- keep in regular touch with local police - the crime prevention officer, crime desk or local intelligence officer. Instruct drivers to secure the cab and where appropriate the load compartment. Where possible, they should lock cab doors when loading or unloading.

- advise them not to talk about their load or intended route in a public place or over the radio. They should be careful when asking people for directions or advice on off-road parking.

If the driver holds the keys to his vehicle when not at work, he should:

- keep them secure at all times;
- never hide them for collection by a relief driver;
- never leave them where they could be copied; and
- make sure there is no way of identifying the keys or the truck from the key ring.

Use security seals on vehicles where appropriate to protect the load. Seals quickly reveal any attempts at tampering through a pre-determined number code or a randomly generated digital seal number. More expensive seals are specially made to withstand violent attack.

Criminals may try to obtain vehicles with your company's livery and staff uniforms as a means of claiming authority to collect goods and/or vehicles. When disposing of vehicles, remove all identifiable livery. Some specialist companies offer a livery removal service.

Use the vehicle registration document to tell DVLA of changes to livery and major components. Pass disposal details relating to scrapped or written off vehicles to DVLA immediately using form V23.

Consignors should offer dangerous goods only to carriers that have been appropriately identified.

In general, you should strictly monitor the storage, issue and return of staff uniforms. When staff leave or exchange uniforms, they should return their old uniforms. Take particular care when issuing staff uniforms to agency drivers.

Sites receiving or consigning high consequence dangerous goods should:

- schedule vehicle deliveries or collections, wherever possible, so that the arriving vehicle can be cross-referenced against the expected vehicle schedule held at the gatehouse; and

- identify the driver and vehicle and give the customer/receiver an estimated time of arrival, which should be within a reasonable period of the intended delivery time.

2.1.3 Communication with staff – high consequence dangerous goods

Make sure that all staff involved with the transport of high consequence dangerous goods understand the need for heightened security measures. Employees are more likely to be reassured than alarmed by such measures.

Open communication allows all staff to report anything suspicious. Consider setting up a 24-hour confidential reporting line.

Investigate any reports of suspicious behaviour and report them to the police by dialing 999. Where appropriate, you should also report them to the Anti-Terrorist Hotline on 0800 789 321.

In certain highly sensitive operations, you may need more formal surveillance systems. Deploy such systems with great sensitivity.

2.1.4 Lorry parking

Transport companies frequently look for details of lorry parking facilities around the country, particularly 'secure' lorry parking. This is a difficult issue, for several reasons.

There is no agreed definition of a 'secure lorry park', even among the police and the insurance industry.

- There are no formal standards for assessing the level of security at a lorry park, or its effectiveness.

- The availability and quality of security measures and other facilities at a lorry park can change rapidly.

The Department for Transport has therefore not been able to publish a list of secure lorry parks all meeting a common standard accepted by government. However, we can provide the best information available from advertised lorry parking facilities. These are listed in the joint International Road Union (IRU) and European Ministers of Transport (ECMT) booklet *Truck Parking Areas in Europe*.

You can download this booklet from the IRU web site www.iru.org/publications

Rather than identify individual lorry parks as secure or otherwise, the IRU/ECMT booklet lists their security features, including:

- 24 hour guarding;
- video system;
- fenced off parking;
- floodlighting; and
- a star security rating.

However, the Department for Transport wishes to emphasise that you should satisfy yourself regarding the level of security at a particular lorry park.

2.1.5 Maintaining security procedures

Security should be part of the daily routine for all staff involved with the transport of dangerous goods. Train your drivers, warehouse and yard staff in the right habits and make security part of their work.

Make sure that you have clearly formulated standards of responsibility and performance. These need to be understood and accepted by everyone involved in vehicle operations. You could instruct new staff in the security measures applicable to their duties as part of their induction training.

Build security duties into every employee's contract of employment. Security should also feature in the job description of every employee involved in the transport of dangerous goods.

Check regularly that drivers understand and use the security equipment fitted to their vehicles. The same goes for security equipment on premises. Many companies have incorporated these principles into staff development programmes.

Companies should also check driving licences regularly - at least every six months. And arrange regular checks to ensure that all security equipment and control measures are functioning correctly. Above all don’t 'fit and forget'.

Keep up-to-date with current security developments and discuss any problems with the company’s security manager (if there is one), local police contacts and others in the industry. Make use of actual events and the experience of others.

2.1.6 Security plans - high consequence dangerous goods

Carriers, consignors and others (including infrastructure managers) engaged in the transport of high consequence dangerous goods should adopt, implement and comply with a security plan.

Your plan should identify and reduce security risks related to the transport of dangerous goods. Implement a plan that is appropriate to your assessed risks. This should take account of the types and amounts of dangerous goods transported and how they are transported.

It should cover at least the following elements:

(a) specific allocations of responsibilities for security to authorised personnel;

(b) records of dangerous goods or types of dangerous goods transported;

(c) review of current operations and assessment of vulnerabilities;

(d) clear statements of security measures, including training and operating practices;

(e) effective and up to date procedures for reporting and dealing with security threats, breaches or incidents;

(f) procedures for evaluating and testing security plans and periodically updating them;

(g) measures to ensure the security of transport information contained in the plan;

(h) measures to ensure that the distribution of transport documentation is limited as far as possible; and

(i) measures to confirm information provided by applicants for positions that involve access to and handling of dangerous goods covered by the security plan.

Consignors should confirm that carriers have a security programme in place.

Carriers, consignors and consignees should co-operate with each other and with the authorities to exchange threat information, apply security measures and respond to security incidents.

2.1.7 Security plans – high consequence dangerous goods – the three steps

There are three steps in drawing up security plans.

Step one – Identify the types of threat.

- What does the news say about the current national and international climate, or current terrorist campaigns?
- What is police advice on the chance of a terrorist attack in the organisation’s area of operations?
- Is there something about the organisation’s building, operations or staff that could attract a terrorist attack?
- Does its location mean that the organisation may suffer collateral damage from an attack on a high-risk neighbour?

Step two – Identify what is to be protected and in particular how it is vulnerable to terrorist attack.

Step three – Identify what you should do to reduce the risk to an acceptable level (it will not be possible to eliminate risk altogether).

At the end of step three you should have a security plan. Note the following important factors:

One person needs to have overall charge of planning. They must have the authority to secure the co-operation of colleagues and if need be to recommend expenditure on protective measures.

Once plans are made:

- follow them; but
- keep them under review so that they reflect changes in buildings and personnel; and
- test them, by holding regular exercises.

2.1.8 Responsibilities – high consequence dangerous goods- appointing people responsible for security

You will need a company security policy and people to carry it out if you are to respond successfully to an actual or potential terrorist attack. If your company has several sites you may wish to appoint one person with overall responsibility for security but also several site-based security co-ordinators.

One person should have full responsibility for the whole security planning process. This person should have sufficient authority to direct the response to security threats. They should also be involved in the planning and design of the site's exterior security, access control and so on. They must be consulted over any new building, renovation work or operation.

Your overall security co-ordinator should share your plans with the police and the other emergency services, particularly regarding evacuation.

A site security co-ordinator should have seven main responsibilities:

1. producing the risk assessment, and the consequent defensive measures and planning;
2. devising and maintaining a search plan;
3. devising and maintaining evacuation plans;
4. deciding on the extent and direction of evacuation;
5. deciding when to re-occupy;
6. liaising with the local police and other emergency services; and

7. arranging staff training, communication cascades and drills, including training for deputies.

The result should be a plan or set of site plans that:

- have been checked with the emergency services;
- have been practised; and
- are regularly audited to ensure that they are still current and workable.

2.1.9 Records - high consequence dangerous goods

You should keep the following information for all transactions involving a scheduled substance. You should keep these records for not less than four years and make them available to the appropriate authorities on request:

a) name and address of the importer / exporter / trader;

b) name and address of the consignee (if known);

c) name and address of any other persons involved in the transaction (that is, the physical movement of the goods) where known;

d) name of the scheduled substance;

e) quantity of the scheduled substance; and

f) date of supply (from the premises).

The legal requirements relating to records may vary from one scheduled substance to another.

Guidelines on identifying suspicious orders or enquiries are available from The British Chemical Distributors and Traders Association or the Chemical Industries Association on request.

2.2 Journeys

2.2.1 Security on the road – drivers

Drivers should report anything unusual to their manager and if appropriate to the police. The sort of things they should report include any irregularity in loading, locking or sealing, or in documents, changes in delivery instructions, or suspicions about people or vehicles.

Advise drivers to:

- where appropriate, remove the ignition keys, lock the cab doors and the vehicle's load space and switch on any alarm or immobiliser whenever they have to leave the vehicle unattended – even when going to pay for fuel or making a delivery;

- refuel on site before setting off whenever possible;

- pre-plan their route and avoid stopping for any reason. The driver should avoid routine stops for cigarettes, newspapers, etc. by stocking up on anything needed for the journey before setting off;

- never leave windows open when away from the vehicle;

- use pre-planned, secure and approved overnight parking facilities where possible. Ask the driver to provide receipts and give the driver a list of overnight parking facilities according to how vulnerable the load is;

- particularly avoid using insecure, casual parking places as a routine practice;

- lock all doors while sleeping in the cab;

- back the vehicle up against a wall or other secure barrier to prevent access to the rear doors if appropriate, but remember the top and sides of the vehicle will remain vulnerable;

- never carry unauthorised passengers;

- never leave the vehicle unattended in a secluded or unlit area at night. Try to keep the vehicle in sight and be able to return to it quickly if it must be left unattended;

- contact base whenever they encounter any delay, problem or change in consignment details. The driver should not change the pre-agreed routing without prior confirmation from base; and

- never leave trailers or containers unattended, whether loaded or not. They should only be left in pre-agreed parking areas with approved security devices fitted and fully operational.

2.2.2 Security on the road – drivers procedures - high consequence dangerous goods

The driver should carry a formal identity document with photograph.

Types of identification may include EU driving licence, passport or a photo ID issued by the driver’s employer or other organisation.

Where this is a change to current practice, inform all organisations making regular deliveries/collections to the site.

Drivers should keep their cab doors and windows closed and locked throughout the journey.

The driver should try to stay with the vehicle at all times unless it is supervised by a competent person.

Drivers should be instructed not to stop on the road unless required to by a police or VOSA (Vehicle and Operator Services Agency) officer in uniform. The driver should then display a ‘dangerous load’ card and talk to the police officer through a closed window. The driver should not get out of their vehicle until the police officer's credentials have been independently verified - see section 2.2.4 ('Dangerous loads card').

2.2.3 Communications and pre-alerts – high consequence dangerous goods

Mobile communications help to prevent crime. They allow the driver to contact base on arrival at an unoccupied site or to report any suspicious activity.

Mobile communications also allow the carrier to keep track of routes and any overnight parking sites used.

Vehicles should be fitted with radios or some other means of two-way communications between the driver and the base.

Instruct the driver to communicate with their operating base at frequent and regular intervals. They should say where they are, what route they are taking and, if appropriate, their estimated time of arrival at their next destination together with confirmation that everything is in order.

Instruct the driver to alert base to any unusual or suspicious activities. Consider giving the driver a password to use when raising the alarm.

Keep details of the routing and nature of high consequence dangerous goods confidential. Consider organising convoy movement and/or covert/overt escorts for such loads.

2.2.4 Dangerous load cards - high consequence dangerous goods

From 1 June 2004, drivers carrying high consequence dangerous goods should carry a dangerous load card. A card is unique to the applicant and will include the applicant's name and address. It does not specify the type of high consequence dangerous goods being carried, the vehicle or the driver. A carrier would need to hold enough cards to cover the maximum number of vehicles carrying high consequence dangerous goods at any one time.

If they are stopped by an officer of the police or VOSA (Vehicle and Operator Services Agency) **and are suspicious** about the validity of the officer, they should produce this card. The UK police and VOSA have approved this procedure. The carrier will need to decide if any load is of high consequence, based on information provided by the consignor. Cards can be obtained by completing an application form. This is available at www.dft.gov.uk/security/dangerousgoods or by requesting a copy by email: DGSECURITY@dft.gsi.gov.uk.

The card tells the police and VOSA that the driver will not open the vehicle until the officer's identity has been verified.

Operators should be aware that for their vehicles to be part of the scheme they should have:

- in-cab communications;

- a working tracking system, where fitted; and

- an effective security plan.

When stopped by a police or VOSA officer in uniform, the driver should:

- Ensure the doors to your vehicle are locked, stay in your cab and secure the parking brake of your vehicle.
- Display the dangerous load card
- If you are in radio contact with your operating centre - Keep in contact, ensure they have the full details of your location and the reason why you have been stopped.
- Ask the officers for identification (talk through the closed window).
- DIAL 999 (The officer will also contact the force control room to inform them of the stop)
- Inform the POLICE control room you are carrying dangerous goods, your location and the identity of the stopping officer.
- If it is a LEGITIMATE STOP - Comply with the instructions of the stopping officer

2.2.5 Reporting security incidents

If there is a security incident, if a vehicle, item of plant or a vehicle's load is stolen or you have suspicions regarding a possible security situation, call the police immediately by dialling 999.

You should also consider reporting such incidents to the anti-terrorist hot line on 0800 789 321.

Key steps - Organisations may already have their own procedures for dealing with the immediate aftermath of a theft or security incident. The following checklist covers the key steps on discovering a theft:

- get details of the plant or vehicle and its load;
- confirm exactly where and when it was last seen;
- report these details to the police. Note the incident number - you may need it again.
- report full details to your insurer(s). Keep copies of all claims submitted.

Give the police more detailed information as soon as you can. Keep vehicle records and information about the load in a safe place.

Further Steps -Tell your drivers and if possible those working for other companies about the stolen vehicle/load so they can look out for it.

There are also databases kept by public and private organisations, some of which offer a facility to register that vehicles have been stolen or to register vehicles and plant owned by the company. Remember, when loads or equipment have been stolen it is essential to put the word out as soon as possible.

TruckWatch schemes

TruckWatch is a crime prevention initiative run by the Freight Transport Association, Road Haulage Association and the police. A number of TruckWatch schemes operate around the country. Schemes raise the profile of crime prevention initiatives in order to reduce theft of goods vehicles.

TruckWatch aims to:

- reduce the theft of goods vehicles and any loads carried on them;
- find stolen vehicles quickly;
- notify police of sightings of stolen goods vehicles as quickly as possible; and
- pass on police information about stolen goods vehicles to drivers and other road transport operators.

TruckPol

TruckPol is a Police Intelligence Desk recording information on all aspects of road freight crime. It was previously known as the Police National Stolen Lorry Load Desk.

TruckPol collates details on the following offences:

- lorry and load theft, including stolen trailers;
- jump-ups - vehicle not moved but entered and all or part of load stolen; and
- trespass on any type of premises and property removed where the thieves would need a Luton-type vehicle or larger to remove goods.

Please report any relevant information to:

Database Co-ordinator
Metropolitan Police

Tel: (0207) 230 7775
Fax (0207) 230 7774
E-mail truckpol@met.police.uk
Web site: www.truckpol.com

Or 07000 878257 TruckPol

2.3 Access

2.3.1 Restricting access - high consequence dangerous goods

Employers can reduce the 'insider' risk by limiting the access individual employees have to key locations, assets and information to that which they need to do their job. This can be done in various ways, depending on the nature of the business.

Examples include:

- physically controlling access to locations housing critical plant, high consequence dangerous goods, IT systems or expensive assets.
- protecting business-sensitive information, whether in hard copy (by, for example, locking it up securely) or soft copy (using access controls on IT systems).
- requiring staff to wear photo ID passes at all times.
- controlling or limiting unsupervised access by contract/agency staff to particular areas.
- stopping contract/agency staff from taking personal possessions into sensitive areas.

2.3.2 Access control - high consequence dangerous goods

Employers should determine whether and how to control access. When securing entry points, consider emergency exits and disabled access.

You also need to establish minimum security requirements, which will potentially prevent tailgating and the possibility of by-passing barriers.

Unexpected vehicles should be refused entry to a site, until their identity and proof of need for entry has been confirmed - see 2.1.2 (Management routines and secure working practices)

3 Assets – introduction

This section highlights effective measures to improve security at sites and on vehicles used for the transport and storage of high consequence dangerous goods.

Good security is a combination of physical measures, sound procedures and the awareness and attitude of managers and employees. Actual measures may vary from site to site, depending on the nature of the business.

All good physical security regimes are based on the 3D principle – deter, detect and delay.

Deter – the overt physical and electronic security measures that might deter a would-be intruder.

Detect – alarm systems, with visual (CCTV) verification, to detect the presence of an intruder.

Delay – physical security measures that delay the intruder long enough to allow a response force to attend.

But if the 3D principle is to work, detection must precede delay.

The Department for Transport recommends that all sites and vehicles, which store or carry dangerous goods should have a minimum level of security to match their vulnerabilities.

3.1. Sites

Sites that handle high consequence dangerous goods classified under the Control of Major Accident Hazards Regulations 1999 regulations as 'top tier' must submit safety reports to the competent authority. These sites are likely to have all aspects of security at the highest level, including personnel. However, you cannot take this for granted. In particular, site location may be a factor. You can get security advice from your local police counter-terrorism security adviser if you think you need it by contacting the police force headquarters.

Carry out a site risk assessment, remembering to consider such contingencies as sabotage to IT systems.

3.1.1 Secure premises

The local police and your insurer will be able to advise on securing premises.
When drawing up security plans, consider the following areas:

- perimeter protection (fences);
- site access and control (barriers);
- surveillance (illumination and CCTV);
- guards;
- intruder detection;
- visitor control;
- limiting the number of key holders;
- staff parking away from the main site;
- controlled access to loading bays, vehicle key storage and control systems;
- personnel and vehicle search procedures; and
- security of any tools or equipment that might help criminals to steal trucks or loads.

The right perimeter illumination should make it easier to identify intruders and vehicles. CCTV surveillance systems should be able to monitor, detect, recognise or identify and should be should be linked with other perimeter intruder detection systems and physical delay measures.

The *Security Service Guide to Producing Operational Requirements for Security Measures* contains detailed guidance on operational requirements for:

- perimeter fencing;
- security lighting;
- CCTV surveillance systems;
- perimeter intruder detection systems;
- physical delay measures; and
- intruder detection systems.

3.1.2 Depot security

Thefts from yard premises remain one of the largest problems for operators. Thieves can be sure that vehicles and often their loads will be on the premises at certain times.

There are a number of ways to improve vehicle security and an effective depot security system will buy time, a vital factor in crime prevention. However, good security is not cheap, so it is important to assess your needs carefully.

Visitors to sites should be scheduled and security personnel should be told of their visit beforehand. They should be accompanied throughout their visit and are the responsibility of the host, who should be a member of staff.

Many sites already require visitors to deposit all electronic equipment at the gatehouse before entering. Consider extending this practice on security grounds.

3.1.3 Searching on entry and exit - high consequence dangerous goods

Some companies have a policy of 'on-the-spot' vehicle and body searches as part of their theft prevention strategy. Where appropriate, it should be a condition of entry to a site that people may undergo a body search. This is particularly important at sites that are involved with pathogens of class 6.2 and explosives of class 1.

Body searches should be witnessed and only trained staff should carry them out. If you feel you need such search procedures, include compliance with them in employees' terms and conditions.

Where there are areas of particular sensitivity and/or risk, employers may also want to consider random searching on entry and exit.

3.1.4 Storage of vehicles

Overnight storage of vehicles in locked buildings is often only practical for light vans. Heavy commercial vehicles need more space, and are generally kept outside. Where vehicles are stored inside, consider the fire risk. Furthermore, the premises can provide cover for the intruders.

Avoid leaving vehicles against fences in the belief that they will be secure. Although the fence will protect the rear doors, the top and sides remain vulnerable. Backing vehicles up against each other provides only limited security to the rear doors. Wherever possible, park vehicles close together with loaded vehicles towards the centre.

3.1.5 Loaded vehicles – high consequence dangerous goods

If high consequence dangerous goods are pre-loaded for departure they are of course more vulnerable if left overnight. Wherever practicable, vehicles should not be left loaded overnight or for any significant period of time before departure. If vehicles have to be pre-loaded for operational reasons, leave them in a secure location, locked, with any alarms or immobilisers set and the keys kept in a safe place.

3.1.6 Fencing

Perimeter fencing is important as it creates the first physical barrier to a site. When considering what type and size of fencing to install, bear in mind local planning authority concerns with regard to the impact on the surrounding environment.

There are several British Standard and commercial fences in common use for site security. But even the most secure types can eventually be scaled, penetrated or burrowed under by a well-prepared intruder who is strong, agile and determined.

The most commonly used fence is the relatively inexpensive chain link fence to BS1722 part 10. However, it is only capable of delaying a reasonably agile intruder for a very short time.

The welded mesh version of BS1722 part 10 or the security pattern (SP) steel security palisade fences to BS1722 part 12 have very useful characteristics. The latter is strong and rigid and offers excellent opportunities for mounting some type of perimeter intruder detection system (PIDS).

However, if a perimeter is next to a public road, footpath or other frequented area, a single fence mounted with a PIDS may signal an alarm so frequently as to be useless. The most practical answer may be a double fence, with the inner fence alarmed, or with an alarmed strip between the two fences. The innermost fence should be the hardest to scale and penetrate to ensure the greatest delay.

At sites with long perimeters, a strong perimeter fence may not be practicable. In such cases, it may be better to concentrate on the areas that need the highest level of protection.

Some operators have installed electric or electrified fences, which can provide both an alarm system and a powerful deterrent.

Remember that criminals will always try to find a way into secure parking areas. You cannot rely on rivers and fields to provide a secure natural boundary.

Many fences such as BS1722 part 10 include strands of barbed wire. Some have barbed wire coils (or concertinas) on top while a few incorporate barbed tape.

Barbed wire, whether in coil or strand form, is much less effective as a deterrent and as a practical defensive measure than the various barbed tapes. However, to avoid legal problems, you should only place barbed tape where it is well out of the reach of passers-by. Furthermore, if you place it on top of a fence to discourage scaling, it must be out of reach of children. This tends to limit its use to fences that cannot be climbed without scaling equipment. Again, to avoid legal problems, it must be obvious to the public that barbed wire or tape is in use.

You must make sure that fences are fitted in accordance with the relevant British Standard and that you set up a maintenance programme.

3.1.7 Mounds and ditches

Mounds around depot boundaries can, if badly planned, actually reduce security. In the worst cases, mounds can lower the effective height of the fences. Ditches are also frequently suggested as a means of greater security. They will not prevent theft from vehicles but they will usually prevent theft of vehicles and trailers.

3.1.8 Gates

Fit gates that are appropriate to the risk. Gates must be compatible with and at least as strong as the perimeter fence. The best, and most expensive, are electric sliding gates that run in "tramways" rather than suspended as these are far more rubust. These will require pedestrian access if not manned 24 hours. An alternative is a good set of metal gates with effective locks.

Other effective measures include gates capable of being double-locked with the hinges welded to prevent them being lifted off. Tap or weld screws wherever possible to prevent their removal. The same applies to the screws and hinges on vehicle locks.

Use a good security padlock of hardened steel. Make sure the bar on any standard padlock you use is as short as possible and shroud the padlock with hardened steel. This makes it more difficult to open using cutting equipment and buys time.

3.1.9 Intruder alarms and verification systems

Use intruder alarms to monitor gates. Also consider using movement detectors. Make sure they are not set at too sensitive a level, but can still detect, for example, someone ramming the depot gates.

Operators should be aware that the police are increasingly refusing to respond to alarms from commercial premises with a history of false alarms, unless the presence of an intruder is verified. There are various means of doing this and a number of intruder verification systems are on the market.

The most expensive consist of a pinhole camera typically situated by a gate or other likely access point. An intruder triggers the camera by breaking the beam from the alarm system. When activated, this sort of system will take photographs at short intervals.

Other cheaper systems work from existing equipment. For instance, you can buy software that connects intruder alarms to a standard PC. When an intruder breaks the beam, the software accesses whichever camera has a view of the area. The previous 10 seconds of recording can then be reviewed from any location where there is a monitor with a telephone link to the system.

Some high-risk sites may require boundary fence intruder protection. There are devices available which trigger a camera when an intruder breaks a beam thrown along a boundary fence.

British Standard BS 4737 covers basic alarm systems for premises and BS 7042 covers high security intruder alarm systems.

3.1.10 Depot lighting

Good lighting is an essential security measure for depots as well as having health and safety benefits. A well-lit perimeter fence, free of concealing vegetation, is a good starting point.

Security lighting:

- deters entry into the area;
- conceals guards and their activities;
- aids visual observation by patrolling guards;
- supports CCTV surveillance;
- illuminates access point(s); and
- makes vehicle searches easier.

Lighting must balance the desire for security with the nuisance that excessive illumination may cause in environmentally sensitive areas.

3.1.11 Camera surveillance

Camera technology is improving all the time. In theory, closed circuit television installed alongside beam movement activators is an excellent means of monitoring a depot. But there are a number of aspects that you need to look at before making any significant investment.

Consider hiring a consultant rather than relying on the installer's advice. This way you will get a system that suits your needs and you avoid the risk of over-specification. A Home Office publication called "CCTV Operational requirements" is available on the web - www.homeoffice.gov.uk/crimpol/police/scidev/publications.html - as a downloadable PDF document. This will give you a clearer idea of how to go about deciding what you actually need in using CCTV.

It is vital that a company has the resources to monitor cameras on a 24-hour basis or at least sets time aside to check recordings. Where cameras are continuously monitored, make sure that monitors are constantly in view of the responsible person and not blocked in any way. Equally, make sure that other staff and visitors cannot see the monitors, and discover the limits of the cameras. Closed circuit television will only be effective if you make sure that cameras give the best possible coverage and that recording equipment is working correctly.

If necessary move cameras regularly so that blind spots do not develop and become known. Avoid these basic errors:

- failure to switch on equipment;
- failure to ensure that enough blank tapes are available before re-recording begins; and
- continued use of worn tapes. Government advice is to change analogue tapes after 12 uses to maintain image quality

Modern digital recording facilities now provide far better images, so use them wherever possible.

Pan and tilt cameras are good for focusing on particular areas. They consist of a moveable camera with a protective cover which allows the user more flexible monitoring.

Dome cameras can have advantages over pan and tilt cameras as the area of cover is greatly improved. They also make it difficult for intruders to tell whether the camera has picked them up.

Consider using fixed cameras on external walls. These are cheaper and there is less to go wrong than with dome or pan and tilt cameras. An ideal system for companies with a limited budget could involve a mixture of camera types.

Cameras set on towers are more versatile than cameras on buildings and will often be preferable to them. Again, dome cameras in such positions will provide the most effective scan of the whole site and can have additional benefits as a management aid. For instance, a dome camera will allow surveillance without showing where it is looking.

Still frame cameras activated by beam movement detectors are an alternative to video cameras.

It is also important to ensure that a reputable company services cameras regularly. There are many companies specialising in service contracts for this sort of equipment. Carefully check the condition of the material protecting the lens. The covering is there to protect the camera from weather damage, but it can itself become damaged over time, distorting the camera's view.

Intruders will often try to avoid detection by pointing cameras skywards, but they may not do the same to cameras on adjacent properties. Consider having a reciprocal arrangement with neighbouring companies. If your premises are located on an industrial estate with limited entry/exit points, consider using cameras covering these points, funded either by companies on the estate or as a joint initiative with the local council. Take care with all cameras near residential sites to avoid any invasion of privacy.

3.1.12 Guards - high consequence dangerous goods

Many companies use in-house guards. The main advantage is employee loyalty, but of course there are disadvantages too. This sort of guarding is expensive and you will need several guards to provide 24-hour security. This is a fixed cost to be balanced against other requirements.

Security could suffer because of the guards' familiarity with colleagues. For the same reason, in-house guards may find 'on-the-spot' searches of their colleagues more difficult than contract guards.

If you choose contract guarding, be alert to the vulnerabilities linked to this option, even when using a well-established firm. There is a danger that contract guards will not know enough about your company's operation and so will fail to recognise risks. If possible, arrange for a pool of guards exclusive to the company who can then become familiar with it.

Some security companies provide travelling guards. Typically they visit premises three times a night. It is important to have a modern clocking-in system so that you can verify when the guards arrived at the premises and how long they stayed. The guards should, of course, vary the times of their visits and they should not build up a routine, as it will soon become obvious to criminals. It is also important to ensure that guards are aware of what may be missing from the site.

In an emergency, the security company should also be able to contact the key holder as soon as possible. The longer the incident reporting process takes, the more time the criminals have to get away and the less likely it is that losses will be recovered.

If you do decide to use third party security, it is important that the contractor provides good quality staff. Check the security company's recruitment procedure.

3.1.13 Raised road blocks and barriers - high consequence dangerous goods

Raised road blocks are a highly effective means of preventing vehicles entering or being driven away without authority but they are very expensive. They must be fitted correctly as the repetitive raising and lowering can break concrete surrounds. Regular checks and maintenance of road blocks are essential and they should be constantly monitored to ensure that legitimate traffic is allowed through.

Many companies use barriers, which are adequate for low risk sites, particularly when they are manned 24 hours. However, most types of barrier can be lifted manually and so offer only limited security.

3.1.14 Key control

Parked vehicles must be locked when at base and the keys kept in a lockable container. This can either be a key case where any missing keys can be noted at a glance or, if required, a secure metal cabinet. Duplicate keys should have similar protection. Remember that the room in which keys are secured should also be protected from unauthorised personnel.

It is very important to have an issuing system, with regular checks on where keys are. If operating from lock-up premises (that is, non-24-hour) it is vital to monitor who has the entrance keys.

Keep the number of staff aware of security arrangements to a minimum. Where possible nominate a limited number of key holders, who should be able to reach the site quickly.

If keys are lost, change locks at once or exchange the vehicle with a similar one kept at another location.

3.1.15 Additional notes on depot security

There are a number of bad practices that can make a depot less secure. For example, pallets stored against fences provide criminals with a ready-made ladder. By the same token, do not leave the yard shunter or any other heavy equipment where it is easily accessible. Criminals could use it to ram fences or break through gates.

Often semi-trailers are left attached to tractor units when parked up in depots. On the one hand this can make the criminals' job much easier. However, if an adequate immobiliser is fitted to the tractor the criminals' job can be made more difficult. If the criminals bring a tractor to take the trailer away, an immovable tractor can frustrate them.

When trailers are disconnected from the units they should be secured with king pin or trailer leg locks. Consider leaving empty curtain-sided vehicles in the depot with the curtains open. This could deter criminals from slashing expensive curtains to see what is inside.

On-the-spot searches of vehicles and staff entering or leaving depots are accepted features of many operations. A vehicle seemingly on a routine journey could be removing goods without authority.

3.2 Vehicles

3.2.1 Vehicle and trailer records

Details of vehicles, trailers and loads should be available quickly in case the police need them. As a minimum, keep a record of the following:

- vehicle registration number/trailer serial number;
- make;
- model;
- body type, for example, dropside, flat bed, curtainsider, solid box, tanker;
- vehicle identification number (VIN);

- engine number;
- gear box number;
- other identification numbers, marks and livery details;
- number of axles;
- special equipment fitted (with serial numbers);
- security devices fitted; and
- mileage.

You should photograph vehicles and items of plant from the front, side and rear. This will help police in issuing descriptions and looking out for the stolen property.

Keep a daily record of each vehicle's movements with precise details of the load and the driver on each occasion. Also note other staff who come into contact with the vehicle or its load, such as the person who loads the goods.

3.2.2 Secure vehicles

Vehicles may be secured by means of a range of additional security measures. Consider the following.

- Use security equipment - it will make vehicles less attractive to criminals. Discuss this with insurers, including 'goods in transit' insurers, vehicle dealers, transport security consultants and security-equipment manufacturers.

- Have security equipment regularly checked by the installer.

- Each vehicle will need different levels and types of security equipment, depending on its use. All vehicles should have some form of immobilisation, if the manufacturer has not already fitted this.

- When buying vehicles, consider the security equipment already fitted and what extras could be fitted.

- Your insurer and the crime prevention officer from the local police can provide specific security advice.

- Trucks are stolen whatever their load might be.

Anti-theft equipment - Manufacturers are producing increasingly sophisticated equipment, often running off the vehicle management system.

Equally, criminals are becoming more ingenious. If nothing else this has raised the quality of vehicle security systems to a level that will defeat the opportunist criminal - providing these systems are armed.

Many anti-theft devices are self-arming and do not rely on the driver remembering to set them. Some equipment gives the driver about 30 seconds to leave the cab after switching off the engine and removing the key from the ignition, and then sets itself automatically. The system will remain armed until de-activated by a high security key, electronic touch sensors or a 'smart card'.

Customer demand - In recent years, car manufacturers have increasingly fitted alarms and immobilisers as standard. This has reduced the number of thefts by opportunists and is often emphasised by manufacturers in the marketing of the car. Theft surveys underline that commercial vehicle operators want manufacturers to fit alarms and immobilisers as standard.

But vehicle manufacturers face a fundamental problem. As soon as a manufacturer fits an anti-theft device as standard, this information is readily available to criminals.

In the past, goods vehicle manufacturers have not fitted anti-theft devices as on-line production options, instead offering retro-fit systems at a dealer level. This is now changing and goods vehicle manufacturers will in future offer anti-theft devices as standard on new models.

Insurers have been increasingly proactive in the specification of anti-theft equipment in commercial vehicles. The insurance industry's testing facility at Thatcham produces a list of approved security devices.

Manufacturers offer factory-fit security systems on many light commercial and some heavy commercial ranges. They are also improving the quality of retro-fit alarms and immobilisers offered by dealers.

If your vehicles are fitted with Thatcham-approved systems you may qualify for reduced insurance. On the other hand, lack of precautions can increasingly lead to insurance companies refusing cover. If a vehicle fitted with a security system is stolen as a result of the device not being activated, insurance companies may refuse to pay out against a claim.

The following pages set out the main types of security systems available for commercial vehicles and how manufacturers are improving vehicle security.

3.2.3 Physical vehicle security

Physical security of commercial vehicles can take the form of additional or stronger high security locks, grilles and the like. It may give either independent security or complement an alarm system. Taken in isolation, physical security can offer a simple and cost-effective solution in low risk situations. It can also be a strong deterrent to the opportunist attacker.

Many security locks depend on the driver to operate them manually. 'Slam locks' are now fast becoming a standard fitting to load space access points in large commercial vehicles. They have proved extremely popular with parcel carriers involved in multiple drops. Drivers only have to close the door and the load is automatically secure. However, any security is only as good as the weakest point. The majority of security devices are in fact stronger than the bodywork to which they are fitted.

The main purpose of the bulkhead dividing the driver/passenger area and the load-carrying compartment in panel vans is to isolate goods in the load compartment. For example, a bulkhead fitted in panel van means that access is only through the side or rear loading doors, which can be secured with additional locks.

Bulkheads come in a variety of materials, such as solid steel, plywood or steel mesh. Correctly fitted mesh bulkheads can give adequate security but still allow thieves to see the goods and may therefore make a break-in more likely. Solid bulkheads are better.

British Standard AU 209 parts 7 and 8 cover physical security.

Immobilisers

Immobilisers aim to render the vehicle or trailer immovable. Immobilisation systems can be used in isolation or integrated into an alarm system. Virtually all insurance approved alarm systems will incorporate, as standard, some form of immobilisation as part of the overall security system.

When choosing an immobilisation system, take into account:

- vehicle type;
- the risk to both vehicle and load; and
- loading and unloading.

Fitting a single system across a fleet, irrespective of use, can create vulnerability.

Steering locks

Steering column locks are incorporated into virtually all vehicles during manufacture. However, professional criminals can quickly overcome factory-fitted steering locks. Other forms of additional security and immobilisation should therefore be fitted.

Fuel valve immobilisers

The most widely used method of vehicle immobilisation prevents the engine being started. In the case of diesel engines, where no electrical ignition system is required, the engine is immobilised by shutting down the fuel injection pump. However, should criminals break into the cab, overcome the steering lock and release the handbrake, they will be able to tow the vehicle away.

Starter motor immobilisation

The starter motor of any type of vehicle can easily be immobilised by altering its wiring. Starter motor immobilisation often forms part of a combined alarm/immobiliser device.

Immobilisation of braking systems

Air brake immobilisation valves have seen many developments since they were introduced. They can now work in conjunction with alarm systems and also incorporate fuel valve and starter motor immobilisation.

Wheel clamps

These are an effective form of immobilisation, especially on the smaller wheels of car-derived and Transit-type vans. Wheel clamps for large commercial vehicles are heavy and cumbersome. Drivers have to fit them and lock them into place, so the risk that they either won't fit them, or that they will fit them incorrectly (particularly at night), is higher than for other vehicle immobilisation devices.

Articulated trailer immobilisation – kingpin/trailer leg locks

By far the most common and effective way to immobilise an articulated trailer is with a kingpin lock. This is a heavy hardened steel clamp or cover, which fits round or over the kingpin and locks it in position. It makes it impossible for the kingpin on the trailer to be coupled with the fifth wheel coupling on the tractor unit.

Fitting kingpin locks can be a difficult and dirty job. Trailer leg locks are an alternative. Both kingpin and trailer leg locks are manually operated devices so the driver has to put them on and lock them into position.

Cameras on vehicles

Cameras are increasingly used on the back of trucks to help the driver manoeuvre the vehicle. These are also a valuable covert measure to monitor the security of the load.

Alarms

Immobilisation does not stop a criminal from vandalising a vehicle or unloading it where it stands. Alarm systems do two things:

- they create a loud sound that provides both a warning and a deterrent; and
- when fitted in conjunction with a vehicle immobiliser, they 'buy time'.

When selecting a vehicle alarm, consider whether you want it to be:

- manual (set by driver) or automatic (self-setting at all times); and
- powered by the vehicle's own battery only or by the vehicle's battery with a back-up facility.

An alarm system powered off the vehicle's own battery may be perfectly sufficient for light commercial vehicles in low risk operations, where the battery is locked under the bonnet. Large commercial vehicles with exposed batteries on the chassis require a back-up facility for alarm systems. There is little point in having an alarm system that can be rendered inoperable merely by disconnecting the battery terminals.

British Standard 6803 calls for a four-hour back-up facility. The majority of insurer-approved equipment provides this.

Key switches turn a system on or off (automatic systems 'pulse' to allow the driver to re-enter the cab or to unload). It is important to use good quality security key switches/pulse devices with a large number of combinations.

British Standards - Operators should study the recommendations in British Standard 6803, which sets out:

- Part I specification for theft prevention devices installed as original equipment;
- Part 2 code of practice for devices installed after vehicle marketing; and
- Part 3 code of practice for the protection of goods in transit.

A further British Standard AU 209 part 7 deals with specification for vehicle cab locking systems. AU 209 part 8 deals with security of the load.

Roof markings - high consequence dangerous goods

The Association of Chief Police Officers has agreed to the wider use of roof markings on HGVs. These help police air support units to identify stolen vehicles. The Department for Transport encourages hauliers to use roof markings, particularly those hauliers who regularly carry high consequence dangerous goods.

Consider using the Police Scientific Development Branch (PSDB) standardised roof marking system, especially for vehicles regularly carrying high consequence dangerous goods. PSDB publication No. 14/99 provides details and you can get a copy by e-mailing psdb.sand.enquiries@homeoffice.gsi.gov.uk

Tractor unit and trailer, tank or container alarm systems - high consequence dangerous goods

In the case of high-risk loads, independent alarm security may be fitted to both the tractor unit and the trailer, tank or container. Where a single shared alarm system covers both the tractor and the trailer, tank or container when they are coupled, the back-up battery may be located on the trailer, tank, or container. Its job is to provide independent protection when the trailer, tank, or container is free-standing. However, this may leave the tractor without any alarm protection at all when separated. In this case, it is important to immobilise the tractor unit.

Tracking systems - high consequence dangerous goods

Tracking systems are not, strictly speaking, anti-theft devices. But they can help in deterring theft and recovering vehicles, where time is often of the essence. Use transport telemetry or other tracking methods or devices to monitor the movement of high consequence dangerous goods where appropriate.

Surveys of vehicle and load theft show an increasing number of operators fitting tracking systems as standard. Tracking system manufacturers also report a rise in interest from operators.

Some tracking system manufacturers offer 24 hour monitoring via a movement sensor linked to the tracking unit. The system manufacturer is then able to alert the owner if the vehicle is illegally moved. This means faster response to theft.

Certain tracking systems offer additional features, including:

- remote vehicle immobilisation;
- door opening recording;
- panic alert systems; and
- geo-fencing facilities.

Geo-fencing constantly monitors the vehicle on a predetermined route or at a known location. Any unauthorised movements will automatically trigger an alert.

Telematic systems offer proven vehicle management benefits, as well as improving security. The benefits include better fuel consumption, enhanced safety and cheaper maintenance. These benefits often mean that telematic systems pay for themselves within a relatively short time.

4. Further security advice

You can get more advice on the security of transporting dangerous goods from the following organisations.

The British Chemical Distributors and Traders Association
Lyme Building
Westmere Drive
Crewe Business Park
Crewe
Cheshire
CW1 6ZD

Tel 01270 258200
Fax 01270 258444
Web site: www.bcdta.org.uk

Chemical Industries Association
Kings Building
Smith Square
London
SW1P 3JJ

Tel 020 7834 3399
Fax 020 7834 4469

Federation of Petroleum Suppliers
3 Slaters Court
Princess Street
Knutsford
Cheshire
WA16 6BW

Tel 01565 631313
Fax 01565 631314
E-mail office@fpsonline.co.uk
Web site www.fpsonline.co.uk

Freight Transport Association
Hermes House
St John’s Road
Tunbridge Wells
Kent
TN4 9UZ

Tel 01892 526171
Fax 01892 534989
Web site: www.fta.co.uk

National Chemicals Emergency Centre
AEA Technology
F6
Culham Science Centre
Abingdon
Oxfordshire
OX14 3ED

Tel 0870 1906621
Web site www.the-ncec.com

Road Haulage Association
Roadway House
35 Monument Hill
Weybridge
Surrey
KT13 8RN

Tel 01932 841515
Fax 01932 852516
Web site: www.rha.net

TruckPol (previously the Police National Stolen Lorry Load Desk)
Metropolitan Police

Tel 020 7230 7775
Fax 020 7230 7774
E-mail truckpol@met.police.uk
Web site www.truckpol.com
Or 07000 878257

Thatcham – The Motor Insurance Repair Research Centre
Colthorpe Way
Thatcham
Berkshire
RG19 4NR

Tel 01635 868 855
Fax 01635 871 346
Web site www.thatcham.org

Police Scientific Development Branch
Sandridge
St.Albans
Hertfordshire
AL4 9HQ

Tel 01727 865 051
Fax 01727 816 233
Email psdb.sand.enquiries@homeoffice.gsi.gov.uk
Web site www.homeoffice.gov.uk/crimpol/police/scidev

For further guidance on setting up good practices and/or assessing potential contractors, see:

- BS7499 Static Site Guarding and Mobile Patrol Services Code of Practice
- BS7858 Security Screening of Personnel employed in a Security Role.
- The British Standards Institute web site: www.bsi-global.com

The Security Industry Authority licences private security contractors. It can also advise on standards for security guards. See their web site at www.the-sia.org.uk

For advice on tested security products and approved installers contact the National Vehicle Security Helpline on 0870 550 2006 or Sold Secure on 01327 264687.

Annex One - Documents Consolidated

1. Joint Chemical Industries Association (CIA) and the British Chemical Distributors and Traders Association (BCDTA): Code of Conduct on Chemical Precursors.

2. Chemical Industries Association: Workforce security: A policy guide for member companies.

3. Security Service: Guide to Producing Operational Requirements for Security Measures.

4. Freight Transport Association: Best Practice Guide to Theft Prevention.

5. Home Office: Steer Clear of Truck Theft - Security Advice for commercial vehicle operators.

6. US Federal Register: DOT RSPA 49 CFR 172 Hazardous Materials Security Requirements.

7. Home Office: Bombs - Protecting People and Property.

8. Home Office: Business as Usual - Maximising business resilience to terrorist bombings.

Annex Two - UN Model Regulations

1.4.1 General provisions

1.4.1.1 All persons engaged in the transport of dangerous goods shall consider security requirements for the transport of dangerous goods commensurate with their responsibilities.

1.4.1.2 Consignors shall only offer dangerous goods to carriers that have been appropriately identified.

1.4.1.3 Transit sites, such as airside warehouses, marshalling yards and other temporary storage areas shall be properly secured, well lit and, where possible, not be accessible to the general public.

1.4.2 Security training

1.4.2.1 The training specified for individuals in 1.3.2 (a), (b) or (c) shall also include elements of security awareness.

1.4.2.2 Security awareness training shall address the nature of security risks, recognising security risks, methods to address and reduce such risks and actions to be taken in the event of a security breach. It shall include awareness of security plans (if appropriate) commensurate with the responsibilities of individuals and their part in implementing security plans.

1.4.2.3 Such training shall be provided or verified upon employment in a position involving dangerous goods transport and shall be periodically supplemented with retraining.

1.4.2.4 Records of all security training undertaken shall be kept by the employer and made available to the employee if requested.

1.4.3 Provisions for high consequence dangerous goods

1.4.3.1 In implementing national security provisions competent authorities shall consider establishing a programme for identifying consignors or carriers engaged in the transport of high consequence dangerous goods for the purpose of communicating security related information. An indicative list of high consequence dangerous goods is provided in Table 1.4.1.

1.4.3.2 Security plans

1.4.3.2.1 Carriers, consignors and others (including infrastructure managers) engaged in the transport of high consequence dangerous goods (see 1.4.1) shall adopt, implement and comply with a security plan that addresses at least the elements specified in 1.4.3.2.2.

1.4.3.2.2 The security plan shall comprise at least the following elements:

(a) specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities;

(b) records of dangerous goods or types of dangerous goods transported;

(c) review of current operations and assessment of vulnerabilities, including inter-modal transfer, temporary tran[illegible]torage, handling and distribution as appropriate;

(d) clear statements of measures, including training, policies (including response to higher threat conditions, new employee/employment verification etc.), operating practices (e.g. choice/use of routes where known, access to dangerous goods in temporary storage, proximity to vulnerable infrastructure etc.), equipment and resources that are to be used to reduce security risks;

(e) effective and up to date procedures for reporting and dealing with security threats, breaches of security or security incidents;

(f) procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans;

(g) measures to ensure the security of transport information contained in the plan; and

(h) measures to ensure that the security of the distribution of transport documentation is limited as far as possible. (Such measures shall not preclude provision of transport documentation required by Chapter 5.4 of these Regulations.)

NOTE: *Carriers, consignors and consignees should co-operate with each other and with appropriate authorities to exchange threat information, apply appropriate security measures and respond to security incidents.*

7.2.4 Security provisions for transport by road, rail and inland waterway

NOTE: *These provisions are in addition to those applicable to all modes of transport as provided in (UN) Chapter 1.4.*

7.2.4.1. Each crew member of road vehicles, trains and inland waterway craft transporting dangerous goods shall carry with them means of identification, which includes their photograph, during transport.

7.2.4.2. When appropriate and already fitted, the use of transport telemetry or other tracking methods or devices shall be used to monitor the movement of high consequence dangerous goods *(see Table 1.4.1 in Chapter 1.4).*

7.2.4.3. The carrier shall ensure the application to vehicles and inland waterway craft transporting high consequence dangerous goods (*see Table 1.4.1 in Chapter 1.4*) of devices, equipment or arrangements to prevent the theft of the vehicle or inland waterway craft or its cargo and shall ensure that these are operational and effective at all times.

7.2.4.4. Safety inspections on transport units shall cover appropriate security measures.

Annex Three - UN indicative list of high consequence dangerous goods

High consequence dangerous goods are those which have the potential for misuse by terrorists, with serious consequences such as mass casualties or mass destruction. The following is an indicative list of high consequence dangerous goods:

Class 1, Division 1.1 explosives

Class 1, Division 1.2 explosives

Class 1, Division 1.3 compatibility group C explosives

Class 1, Division 1.5 explosives

Class 2.1 flammable gases in bulk[1]

Class 2.3 toxic gases (excluding aerosols)

Class 3 flammable liquids in bulk[1] of packing groups I[2] and II[3]

Class 3 and Class 4.1 desensitised explosives

Class 4.2 goods of packing group I[2] in bulk[1]Class 4.3 goods of packing group I[2] in bulk[1]

Class 5.1 oxidizing liquids in bulk[1] of packing group I[2]

Class 5.1 perchlorates, ammonium nitrate and ammonium nitrate fertilisers, in bulk[1]

Class 6.1 toxic substances of Packing Group I[2]

Class 6.2 infectious substances of Category A

Class 7 radioactive material in quantities greater than 3,000 A_1 (special form) or 3,000 $A_{2,}$ as applicable, in Type B and Type C packages.[4]

Class 8 corrosive substances of packing group I[2] in bulk[1]

[1] Bulk means carriage in quantities above 3,000l in either UN portable tanks or UN bulk containers, as defined in 1.2.1 of the UN Model Regulations, or tank-vehicles, demountable tanks or tank containers, as defined in 1.2.1 of the European Agreement Concerning the International Carriage of Dangerous Goods by Road.

[2] Substances presenting high danger as defined in the European Agreement Concerning the International Carriage of Dangerous Goods by Road

[3] Substances presenting medium danger as defined in the European Agreement Concerning the International Carriage of Dangerous Goods by Road

[4] For purposes of non-proliferation of nuclear material, the Convention on Physical Protection of Nuclear Material must be applied - supported by IAEA INFCIRC/225(Rev.4).