INF.10

ECONOMIC COMMISSION FOR EUROPE

INLAND TRANSPORT COMMITTEE

Working Party on the Transport of Dangerous Goods
(Geneva, 9-12 May 2005, agenda item 9)

Industry Security Guidelines

Transmitted by AISE, CEFIC, CEPE, CLECAT, ECTA, EFMA, FECC, FIATA, IRU

At an informal ADR Workshop on Security in London, 6-8 September 2004, industry made a commitment to develop Industry Guidelines for the Security of the Transport of Dangerous Goods by Road.

Nine associations (representing a large part of manufacturing, transport, distribution and forwarding industries involved in the transport of dangerous goods), listed on page 2 of the attached document, have been working together to develop these Guidelines.

The Guidelines have been developed by a group of industry experts from these associations, who have made use of already existing guidelines in UK, Germany and in a number of sectors of the industry.

The Guidelines provide companies, involved in the transport of dangerous goods by road, with a list of options on how the requirements of the new ADR Chapter 1.10 can be met. It is however up to each company to select the most appropriate and effective means from this toolbox, commensurate with the risks involved, and taking into account the specific conditions in which it operates.

These Guidelines are provided as information to WP.15 but it is certainly not intended that National Competent Authorities would include all options as binding requirements in national legislation. These Guidelines should rather be used as a basis for consultation between the Authorities and the industry involved.

INDUSTRY GUIDELINES FOR THE SECURITY OF THE TRANSPORT OF DANGEROUS GOODS BY ROAD

April 2005

TABLE OF CONTENTS

Disclaimer

This document is intended for information only and sets out guidelines for the security of the transport of dangerous goods by road. The information contained in these Guidelines is provided in good faith and, while it is accurate as far as the authors are aware, no representations or warranties are made about its completeness. It is not intended to be a comprehensive guide to all detailed aspects of the security of the transport of dangerous goods by road. No responsibility will be assumed by the authors in relation to the information contained in these Guidelines.

AISE (International Association for Soaps, Detergents and Maintenance Products) www.aise-net.org
CEFIC (European Chemical Industry Council) www.cefic.org
CEPE (European Council of the Paint, Printing Ink and Artists' Colours Industry) www.cepe.org
CLECAT (European Association for Forwarding, Transport, Logistics and Customs Services) www.clecat.org
ECTA (European Chemical Transport Association) www.ecta.be
EFMA (European Fertilizer Manufacturers Association) www.efma.org
FECC (European Association of Chemical Distributors) www.fecc.org
FIATA (International Federation of Freight Forwarders' Associations) www.fiata.com
IRU (International Road Transport Union) www.iru.org

INTRODUCTION

Following the events of September 11 2001, international legislators considered it necessary to develop and implement measures regarding security for the transportation of goods by road, rail and inland waterways against possible terrorist risks.

On the basis of relevant UN recommendations security provisions – as opposed to classic safety provisions – have been listed in a new ADR Chapter 1.10 and address all parties involved in the transport chain.

These measures take effect on January 1st, 2005 and must be implemented at the end of the usual 6-months transition period on July 1st, 2005. However, companies affected should not rely on these dates but should start preparations as soon as possible. They should be aware that the legislators expressly stated the aims of the regulations is the minimisation of the risk of misuse of dangerous goods for terrorist purposes through which persons, property or the environment might be endangered. Absolute protection cannot be achieved in the transportation of dangerous goods.

Security measures should be an integral part of the safety and quality management system of every company involved with the transport of dangerous goods.

The general requirements of ADR Chapter 1.10 are mandatory. However, the specific ways they are addressed will depend upon the individual circumstances of the undertakings in a particular transport chain and their assessment of the risks and possible outcomes. For example, the measures taken by a company located in a residential area or adjacent to a strategic transport corridor could be very different to one located or operating in open country.

These Guidelines have been designed by industry to provide as comprehensive a range of technical and operational options as possible, from which users can select their optimum mix of options to achieve compliance with the regulatory requirements of Chapter 1.10.

These Guidelines are NOT a prescriptive list of every action a company must take to meet the regulations. Rather it sets out the likely outcomes of a range of possible interventions, whereby the individual comments can only be properly understood in the context of the relevant regulation texts.

These Guidelines are of a voluntary and indicative nature. Companies will need to decide individually how to apply these Guidelines according to their own judgement, as long as their actions are in conformity with the applicable law. In addition, they should be particularly attentive to comply with the legislation applying to data protection/privacy, when conducting actions in this field.

The regulations of chapter 1.10 do not apply to the carriage of limited quantities and quantities below the levels of subsection 1.1.3.6.3 ADR.

It is important to note that in terms of security provisions 1.1.3.6.3 also applies to tank and bulk transport by road vehicles.

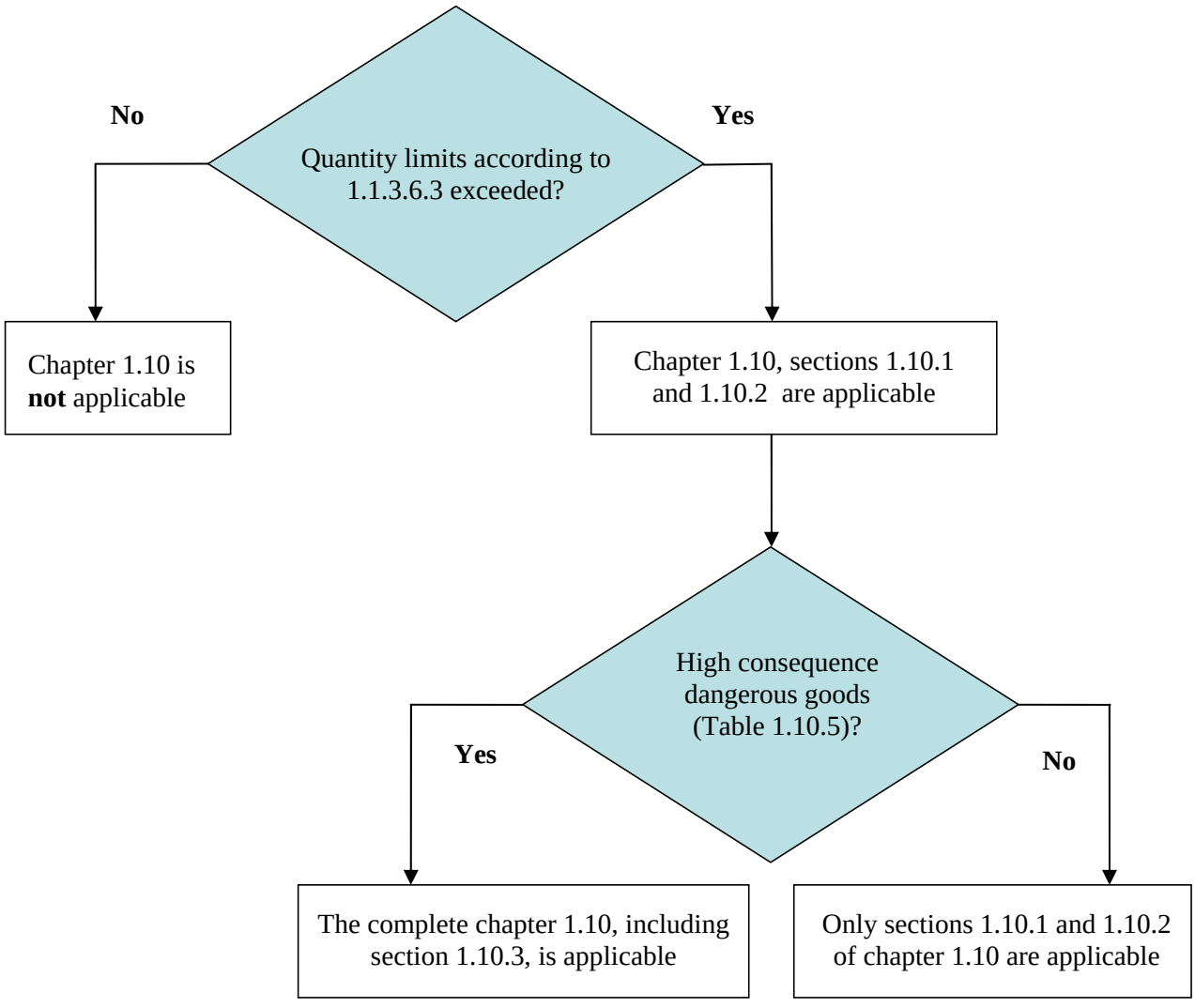
Chapter 1.10 is not applicable for certain goods which are listed in table 1.10.5 as high consequence dangerous goods (e.g. Potassium Cyanide, UN 1680, class 6.1, Packing group I) with a quantity limit of 0 Kg per packaging. The levels of subsection 1.1.3.6.3 take precedence over the quantity limits prescribed in table 1.10.5 where the limits in table 1.10.5 are lower than in subsection 1.1.3.6.3**.**

The quantity limitations refer to each transport unit. This does not prevent the total annual quantity carried or handled by a company being in excess of this limit. This makes sense as any misuse would refer to an individual act of carriage.

If the quantity limits are exceeded, the regulations of 1.10 sections 1.10.1 and 1.10.2 apply. In the case of high consequence dangerous goods, section 1.10.3 also applies.

Section 1.10.3 introduces specific and more onerous special rules for dangerous goods with a higher danger potential, dealing not only with the general misuse and related dangers but specifically with the misuse for terrorist purposes and their potentially serious consequences.

The following flow chart shows the sequence of decisions to be taken (quantity relates to packaged goods as well as to carriage in tanks and bulk containers):



GUIDELINES

In these Guidelines the text of the provisions of the new ADR Chapter 1.10 is presented in blue characters and has been shaded in blue. It always precedes the relevant comments.

CHAPTER 1.10

SECURITY PROVISIONS

NOTE : *For the purposes of this Chapter, security means measures or precautions to be taken to minimise theft or misuse of dangerous goods that may endanger persons, property or the environment.*

1.10.1 General provisions

1.10.1.1 All persons engaged in the carriage of dangerous goods shall consider the security requirements for the carriage of dangerous goods set out in this Chapter commensurate with their responsibilities.

Each person involved ought to be aware of the misuse potential of dangerous goods. Everyone has to observe the relevant legislation in accordance with their responsibilities within their company organisation. This applies equally for example to staff of consignors, loaders, carriers, unloaders and consignees.

Reliable and responsible employees are central to making sure that security measures work effectively. Documentary evidence of the background and experience of anyone being recruited should be obtained.

Companies should ensure all employees who are involved with the transport of dangerous goods hold verifiable:

- licences, certificates and operating documents where applicable; and
- any necessary work permits, etc

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

In conformity with any applicable national legislation, employers should check the employment record of everyone involved in the transport of dangerous goods on initial recruitment and licences etc at regular intervals.

The candidate should be asked for the following information:

- Full name;
- Address;
- Date of birth;
- National, governmental or other unique personal identifying number where appropriate;
- Details of any past criminal convictions (where this is allowed by law);
- Full details of references (where applicable).

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

- If possible direct contact should be made with the previous employer(s) to discuss the applicant's work record and character.
- When checking references by phone, the number supplied by the applicant should be checked e.g. from a telephone directory or enquiries service.
- Open references such as 'to whom it may concern' should not be accepted.
- Confirmation in writing may be obtained from employers, educational authorities, and so on.
- A progress sheet to record all the actions taken should be kept.
- The identity should be checked by asking to see a passport, an official photo ID (such as a driving licence incorporating a photograph), utility bills sent to the applicant's address and so on.
- In the absence of an identity card a recent photograph of the applicant should be obtained and he/she should sign it in the presence of a company representative
- Driving licences should be checked thoroughly: examine the licence closely for signs of alteration, discolouration or erasure. It should be made sure that the background colours are correct and intact. Stained or damaged licences should raise suspicions and endorsements should be checked for. The licence should be copied and the copy kept on file.

Much of this information can be gathered as part of a well structured interview.

1.10.1.2 Dangerous goods shall only be offered for carriage to carriers that have been appropriately identified.

No particular actions are required if there is a regular business relationship with the carrier since the identity of the business partner is known. However, there should still be regular auditing of procedures adopted by the company offering dangerous goods for carriage.

When starting a new business relationship the reliability of the partner should be ascertained. Each company has to decide individually on how to proceed with this, for example, based upon their own criteria or using existing systems such as SQAS (Safety and Quality Assessment System), the CDI's (Chemical Distribution Institute) Marine Packed Cargo scheme (MPC) or the traditional ISO standardisation systems.

Goods may only handed over for carriage if the right to receive the goods has been ascertained by suitable measures

Contractors

Businesses use contractors or agencies to provide a growing range of services. But contractors may create new vulnerabilities and expose businesses to a greater 'insider' threat than they would face if relying on directly recruited employees. 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 an appropriate code of practice for the 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.

Companies 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 procedures are in place to confirm that a person sent by a contractor or agency is indeed the individual who turns up.

In the absence of official ID documents, this may be achieved by the following procedures: for example

- Requiring the contractor or agency to provide in advance a photo of the individual, authenticated by them. This can be compared with the person who turns up at the company’s premises before he/she is let in.
- Requiring the contractor or agency to provide their own photo ID, which can be checked on each entry
- If directly employed staff are provided with a photo ID, extending this requirement to contract staff. Ideally these passes should be retained between visits. On each visit, the contractor or agency staff member should be compared with their photograph before the pass is handed over.
- Having an agreed substitution procedure for contract staff that is 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.

1.10.1.3 Areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshalling yards used for the temporary storage during carriage of dangerous goods shall be properly secured, well lit and, where possible and appropriate, not accessible to the general public.

"Temporary storage" does not, and should not encompass overnight parking or stops en-route. "Parking" is not the same as "storage".

Areas for the temporary storage during carriage are areas where interruptions of transport are intended and take place regularly (e.g. stops made necessary by the conditions of carriage as well as periods involved in order to change the mode of transport – transshipment as well as stops necessitated by the circumstances of transport). Interruption in this sense is not stopping or parking e.g. at a service area. The regulatory requirements for parking and supervision are defined in ADR section 8.4

"Properly secured" means those areas where access is controlled by adequate technical or organizational measures (e.g. clear-cut regulations for access by which the access/stay of unauthorized persons is prohibited).

"Well lit" are those areas in particular where a relevant obligation already exists under industrial safety provisions (for workers). Irrespective of this, adequate technical monitoring systems (e.g. infrared systems) may be used.

"Where possible and appropriate, not accessible to the general public" means that access is prohibited especially by organizational measures (e.g. regulations for access for persons and vehicles – also via rail -, no public access roads). In general physical access barriers (e.g. fences) and site patrols are not necessary if unauthorized persons can be clearly identified and kept out by other measures.

Restricting access

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.

See Annex I for a list of technical options to secure temporary storage areas.

1.10.1.4 Each crew member of a vehicle carrying dangerous goods shall carry with them means of identification, which includes their photograph, during carriage.

For this it is recommended not only to ascertain the identities of the crew members of the road vehicle or vessel but also to record at least their names. This may be done for example by entering the respective data into the company-internal checklists for the implementation of section 7.5.1 ADR (see also comments on 1.10.1.5). This measure is primarily intended to prevent unauthorized persons from picking up dangerous goods. Spot checks should also be considered by comparing the information with that provided by the carrier prior to the collection or delivery of the dangerous goods**.**

1.10.1.5 Safety inspections in accordance with 1.8.1 and 7.5.1.1 shall cover appropriate security measures.

The obligations in accordance with section 7.5.1 ADR are thus extended to security aspects. Suitable measures of the companies for security checks on incoming vehicles before entering company premises might be:

- Using random but recorded order numbers for unloading and loading
- Identifying crew by official ID-documents. In this context attention is drawn to the need of strict observance of the requirements of section 8.3.1 ADR (carrying of passengers)
- Checking the driver's qualifications according to road haulage legislation (where applicable).
- Identifying vehicles based on vehicle documents
- Checking the loading and unloading documentation as well as the consignee's address
- Recording of vehicle crew, vehicle, load and destination

1.10.1.6 The competent authority shall maintain up-to-date registers of all valid training certificates for drivers stipulated in 8.2.1 issued by it or by any recognized organization.

No further guidance is required since this is the duty of the competent authorities.

1.10.2 Security training

1.10.2.1 The training and the refresher training specified in Chapter 1.3 shall also include elements of security awareness. The security refresher training need not be linked to regulatory changes only.

1.10.2.2 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 and duties of individuals and their part in implementing security plans.

Companies should provide security awareness training for everyone involved in the carriage of dangerous goods. They should periodically supplement initial training with refresher training.

The training should deal with:

- The nature of security risks;
- Recognising security risks;
- How to minimise security risks;
- What to do in the event of a security breach.

Drivers and other relevant categories of personnel should be briefed 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/or load.

1.10.3 Provisions for high consequence dangerous goods

1.10.3.1 "High consequence dangerous goods" are those which have the potential for misuse in a terrorist incident and which may, as a result, produce serious consequences such as mass casualties or mass destruction. The list of high consequence dangerous goods is provided in Table 1.10.5.

1.10.3.2 *Security plans*

A substantial additional measure is the creation and implementation of security plans.

The content of a security plan should be based on the general situation of the company, not on individual transports.

Where elements of the security plan are already in place by reason of other legal obligations or within quality systems, reference to these elements can be made in the security plan.

1.10.3.2.1 Carriers, consignors and other participants specified in 1.4.2 and 1.4.3 engaged in the carriage of high consequence dangerous goods (see Table 1.10.5) shall adopt, implement and comply with a security plan that addresses at least the elements specified in 1.10.3.2.2.

It should be stressed that everyone concerned with chapters 1.4.2 and 1.4.3 ADR must work out security plans. The individual parts of a security plan can only reflect the respective activities of the company concerned. A company that, although cited in sections 1.4.2 and 1.4.3 as participant, is not concerned with the physical handling of dangerous goods with high consequences (forwarding agent not acting as carrier or without own loading/unloading sites or without a warehouse) needs to limit the implementation to organisational measures.

There are three steps in drawing up security plans.

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

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

Completing the three steps should result in a security plan.

A template for drawing up a security plan is attached in Annex IV

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:

- They should be followed
- They should be kept under review so that they reflect changes in buildings and personnel;
- They should be tested by holding regular exercises.

The plan should identify and reduce security risks related to the transport of dangerous goods. Implement a plan that is appropriate to the assessed risks. This should take account of the types and amounts of dangerous goods transported and how they are transported.
All organisations involved in the carriage of high consequence dangerous goods should satisfy themselves that their partners have a security plan 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.

1.10.3.2.2 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;

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

A company security policy is needed as well as people to carry it out if it is to respond successfully to an actual or potential terrorist attack. If a company has several sites it 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.

The overall security co-ordinator should share the 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 site 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;
7. Arranging staff training, communication cascades and drills, including training for deputies.

The result should be a plan or set of site plans, which should be coordinated at company level, that:

- have been practised; and
- are regularly audited to ensure that they are still current and workable.

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

A summary list of the type of dangerous goods with a high danger potential carried (e.g. like table 1.10.5) must be kept, without the need to record quantities.

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

Where national guidelines are available on what constitutes suspicious orders or enquiries, these should be followed.

(c) review of current operations and assessment of security risks, including any stops necessary to the transport operation, the keeping of

dangerous goods in the vehicle, tank or container before, during and after the journey and the temporary storage of dangerous goods during the course of intermodal transfer or transshipment between units;

Security on the road – drivers' procedures – high consequence dangerous goods

Security plans should consider whether drivers should be encouraged to 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 the police or other regulatory officer in uniform.

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, they should be left in a secure location, locked, with any alarms or immobilisers set and the keys kept in a safe place.

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.

(d) clear statement of measures that are to be taken to reduce security risks, commensurate with the responsibilities and duties of the participant, including:

- Training;

The increase in alertness to the possible misuse of dangerous goods with a high danger potential must be higher here than in section 1.10.2.
The contents of a training course could comprise the following:

- Type of risk,
- Detection of a risk,
- Procedures for the minimization of such risks,
- Measures to be taken when company specific security rules have been broken,

- Awareness of the security plan in line with the responsibilities assigned
- Obligations of individuals under this plan.

- security policies (e.g. response to higher threat conditions, new employee/employment verification, etc.);

Should the company receive information about an increased threat their staff must be informed without delay. If necessary, suitable measures should be agreed with suppliers and customers.

With regard to checking applicants prior to employment the usual means should be used, e.g., references, CV's documenting employment history, police attestation, etc. (see also 1.10.1.2 above).

- operating practices (e.g. choice/use of routes where known, access to dangerous goods in temporary storage (as defined in (c)), proximity to vulnerable infrastructure etc.);

Road haulage does not usually follow prescribed routes in urban environments in central Europe. Indeed following the same route consistently could add to risks. However consideration should be given to establishing a route plan for a specific journey, so that any deviation can be easily ascertained and tracked.

Current legislation regarding risk prevention should also be considered.

See Annex II for a more detailed list of management routines and operating practices for reducing the security risk

- equipment and resources that are to be used to reduce security risks;

Existing employees - high consequence dangerous goods

There are obvious sensitivities when it comes to directly employed staff. In the vast majority of cases, the 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.

There is a need to check existing employees who work on sensitive sites in order to ensure the integrity of the overall system.

Information on existing employees should be maintained to the same standard as for new employees.

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. This information needs regular checking and updating.

If this process provokes any security-related questions they should be raised 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 with dangerous goods and the serious view taken of dishonesty, irresponsibility or negligence.

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 the avoidance of theft of their load and vehicle 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.

Access control - high consequence dangerous goods

Employers should determine whether and how to control access. When securing entry points, emergency exits and disabled access should be considered.
There is also a 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

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 it is felt that such search procedures are needed, compliance with them should be included 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.

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

In order to meet the requirements for reporting, existing alarm and emergency procedures may be used.

Reporting security incidents

If there is a security incident, if a vehicle, item of plant or a vehicle's load is stolen or if a possible security situation is suspected, the police should be called immediately.

Key steps

Companies 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:

- Getting details of the plant or vehicle and its load;
- Confirming exactly where and when it was last seen;
- Reporting these details to the police and noting the incident number - this may be needed again.
- Reporting full details to the insurer(s) and keeping copies of all claims submitted.

The police should be given more detailed information as soon as possible. Vehicle records and information about the load should be kept in a safe place.

Further Steps: drivers employed by the company and if possible those working for other companies should be told 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. It should be remembered that, when loads or equipment have been stolen it is essential to put the word out as soon as possible.

Industry Monitoring

Truck watch schemes may be run on a national basis, they aim 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.

Police Monitoring

Police Intelligence Desks may record information on all aspects of road freight crime.

They may collate 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 panel van or larger vehicle to remove goods.

Any relevant information should be reported to the appropriate Authorities

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

The required procedures may be integrated into existing safety and quality management systems and existing management procedures should be extended appropriately.

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

The plan and the transport information should be made available to staff on a “need to know” basis.

(h) measures to ensure that the distribution of information relating to the transport operation contained in the security plan is limited to those who need to have it. Such measures shall not preclude the provision of information required elsewhere in ADR.

A security plan showing specific risk potentials represents a highly sensitive document that should only be accessible to uniquely identified individuals. This requires special measures that need to be recorded in the security plan. It also includes IT security

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

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.

Drivers should be instructed 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.

They should also be instructed to alert base to any unusual or suspicious activities. Consideration should be given to providing the driver with a password to use when raising the alarm.

Details of the routing and nature of high consequence dangerous goods should be kept confidential. Organising convoy movement and/or covert/overt escorts for such loads should be considered.

If relevant information becomes known to the company it should liaise with public authorities, suppliers and customers to arrange suitable counter measures (see also 1.10.3.2.2. d)).

Communication with staff – high consequence dangerous goods

Organisations should ensure 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. Setting up a 24-hour confidential reporting line could be considered.

Any reports of suspicious behaviour should be investigated and reported to the appropriate authorities.

In certain highly sensitive operations, there may be a need for more formal surveillance systems. Such systems should be deployed with great sensitivity.

1.10.3.3 Devices, equipment or arrangements to prevent the theft of the vehicle carrying high consequence dangerous goods (see Table 1.10.5) or its cargo, shall be applied and measures taken to ensure that these are operational and effective at all times. The application of these protective measures shall not jeopardize emergency response.

NOTE: *When appropriate and already fitted, the use of transport telemetry or other tracking methods or devices should be used to monitor the movement of high consequence dangerous goods (see Table 1.10.5).*

For the implementation of this regulation for road haulage reference is made to the requirements of chapter 8.4 ADR (regulations for the monitoring of vehicles).

Security on the road-

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.

Drivers should be advised 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;
- 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.

See Annex III for a list of technical options for preventing theft of, or interference with, vehicles or loads during transport operations.

1.10.4 In accordance with the provisions of 1.1.3.6, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in packages on a transport unit do not exceed those referred to in 1.1.3.6.3. In addition, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in tanks or in bulk on a transport unit do not exceed those referred to in 1.1.3.6.3.

See introduction

1.10.5 High consequence dangerous goods are those listed in the table below and carried in quantities greater than those indicated therein.

Table 1.10.5: List of high consequence dangerous goods

Class	Division	Substance or article	Quantity		
			Tank (*l*)	Bulk (kg)	Packages (kg)
1	1.1	Explosives	[a]	[a]	0
	1.2	Explosives	[a]	[a]	0
	1.3	Compatibility group C explosives	[a]	[a]	0
	1.5	Explosives	0	[a]	0
2		Flammable gases (classification codes including only the letter F)	3000	[a]	[b]
		Toxic gases (classification codes including letters T, TF, TC, TO, TFC or TOC) excluding aerosols	0	[a]	0
3		Flammable liquids of packing groups I and II	3000	[a]	[b]
		Desensitized explosives	[a]	[a]	0
4.1		Desensitized explosives	[a]	[a]	0
4.2		Packing group I substances	3000	[a]	[b]
4.3		Packing group I substances	3000	[a]	[b]
5.1		Oxidizing liquids of packing group I	3000	[a]	[b]
		Perchlorates, ammonium nitrate and ammonium nitrate fertilizers	3000	3000	[b]
6.1		Toxic substances of packing group I	0	[a]	0
6.2		Infectious substances of Category A	[a]	[a]	0
7		Radioactive material	3000 A_1 (special form) or 3000 A_2, as applicable, in Type B or Type C packages		
8		Corrosive substances of packing group I	3000	[a]	[b]

[a] *Not relevant.*

[b] *The provisions of 1.10.3 do not apply, whatever the quantity is.*

***NOTE**: For purposes of non-proliferation of nuclear material the Convention on Physical Protection of Nuclear Material applies to international transport supported by IAEA INFCIRC/225(Rev.4).*

ANNEX I

Technical options for securing temporary storage areas

Lorry parking

There may be no national definition of a ‘secure lorry park’; where one is available, it should be used.
There may be 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.
Operators should satisfy themselves regarding the level of security at any lorry park to be used.

A booklet on lorry park security can be downloaded 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;
- Star security rating.

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 several guards will be needed 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 contract guarding is chosen, it is necessary to 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 the company's operation and so will fail to recognise risks. If possible, arrangements should be made for a pool of guards, extern to the company, who can then become familiar with it.

Some security companies provide travelling guards. Typically they visit premises several times a night. It is important to have a modern clocking-in system so that it can be verified 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 it has been decided to use third party security, it is important that the contractor provides good quality staff. Therefore the security company's recruitment procedure should be checked.

Secure premises

The local police and the company's insurer should be able to advise on securing premises.

When drawing up security plans, the following areas should be considered:

- Perimeter protection (fences);
- Site access and control (barriers);
- Surveillance: illumination and Closed Circuit Television (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;
- 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.

Advice on more detailed measures may be available from National Security Services; e.g. the UK *Security Service Guide to Producing Operational Requirements for Security Measures* (http:// www.dft.gov.uk/stellent/groups/dft_transsec/documents/downloadable/dft_transsec_027285.pdf) contains detailed guidance on operational requirements for:

- Perimeter fencing;
- Security lighting;
- CCTV surveillance systems;
- Perimeter intruder detection systems;
- Physical delay measures;
- Intruder detection systems.

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 the 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. Extending this practice on security grounds should be considered.

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, the fire risk should be considered. Furthermore, the premises can provide cover for the intruders.

Leaving vehicles against fences, in the belief that they will be secure, should be avoided.. 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, vehicles should be parked close together with loaded vehicles towards the centre.

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, any local planning authority concerns with regard to the impact on the surrounding environment should be borne in mind.

There are several types and standards of 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. However, it is only capable of delaying a reasonably agile intruder for a very short time.

The welded mesh version or the security pattern (SP) steel security palisade fences 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.

Criminals will always try to find a way into secure parking areas. It is not possible to rely on rivers and fields to provide a secure natural boundary.

Many fences 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, barbed tape should only be placed where it is well out of the reach of passers-by. Furthermore, if placed 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.

Fences should be fitted in accordance with the relevant standard and a maintenance programme should be set up.

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.

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, ones are electric sliding gates that run in "tramways", as these are far more robust, than suspended gates. 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. Screws should be tapped or welded wherever possible to prevent their removal. The same applies to the screws and hinges on vehicle locks.

A good security padlock of hardened steel should be used and it should be made sure that the bar on any standard padlock used is as short as possible and that the padlock is shrouded with hardened steel. This makes it more difficult to open using cutting equipment and moreover buys time.

Intruder alarms and verification systems

Intruder alarms should be used to monitor gates. Movement detectors could also be considered. They should not be set at too sensitive a level, but should still be able to 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 available.
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, software can be bought 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.

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);
- Makes vehicle searches easier.

Lighting must balance the desire for security with the nuisance that excessive illumination may cause in environmentally sensitive areas where infra red illumination may be more appropriate.

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 need to be looked at before making any significant investment.

A consultant could be hired rather than relying on the installer's advice. In this way a system that suits the needs is more likely to be installed, and will avoid the risk of over-specification. A UK Home Office publication called "CCTV Operational requirements" is available on the internet - www.homeoffice.gov.uk/crimpol/police/scidev/publications.html - as a downloadable PDF document. This gives a clearer idea of how to go about deciding what is actually needed 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, monitors should constantly be in view of the responsible person and not blocked in any way. Equally, other staff and visitors must not be able to see the monitors, and therefore the limits of the cameras should be established. Closed circuit television will only be effective if cameras give the best possible coverage and if the recording equipment is working correctly.
If necessary, cameras should be moved regularly so that blind spots do not develop and become known. The following basic errors should be avoided:

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

Modern digital recording facilities now provide far better images, so wherever possible these should be used.

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.

The use of fixed cameras on external walls should be considered. 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. The condition of the material protecting the lens should be carefully checked. 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. Having a reciprocal arrangement with neighbouring companies should be considered. If premises are located on an industrial estate with limited entry/exit points, consideration should be given to using cameras covering these points, funded either by companies on the estate or as a joint initiative with the local council. Extreme care should be taken with all cameras near residential sites in order to avoid any invasion of privacy.

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, the yard shunter or any other heavy equipment should not be left 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. Consideration should be given to 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.

ANNEX II

Management routines and operating practices for reducing the security risk

Management routines

There are a number of management routines that can be adopted to improve security.

Management should:

- Constantly review operational procedures;
- Consider possible risks and always bear security measures in mind;
- Ensure that employees are given the confidence to report concerns and must know that their employer will take their reports seriously and treat them confidentially
- 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. Management should develop secure practices for controlling keys to vehicles and premises. 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
- Where possible, vary routes and drivers to avoid regular patterns developing;
- 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 drivers 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.

Where appropriate, security seals on vehicles to protect the load should be used. 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 a company's livery and staff uniforms as a means of claiming authority to collect goods and/or vehicles. When disposing of vehicles, all identifiable livery should be removed. Some specialist companies offer a livery removal service.

The vehicle registration document should be used to inform regulatory/licensing authorities of changes to livery and major components. Disposal details relating to scrapped or written off vehicles should be passed to authorities immediately, using an appropriate form.

In general, the storage, issue and return of staff uniforms should be strictly monitored. When staff leave or exchange uniforms, their uniforms should be returned. Particular care should be taken 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;
- 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.

Operating practices

Security should be part of the daily routine for all staff involved with the transport of dangerous goods. Drivers, warehouse and yard staff should be trained in the right habits and security should be made part of their work.

There need to be clearly formulated standards of responsibility and performance. These need to be understood and accepted by everyone involved in transport operations**.** As part of their induction training, new staff should be instructed in the security measures applicable to their duties.

Security duties should be built 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.

Regular checks should be carried out in order to verify 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. Regular checks should be arranged to ensure that all security equipment and control measures are functioning correctly.

There is a need to keep up-to-date with current security developments and to discuss any problems with the company's security manager (if there is one), local police contacts and others in the industry, so that use can be made of actual events and the experience of others.

ANNEX III

Technical options for preventing the theft of, or interference with, vehicles or loads during transport operations

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 and the room in which keys are secured should also be protected from access by 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.

The number of staff aware of security arrangements should be kept to a minimum. Where possible a limited number of key holders should be nominated and they should be able to reach the site quickly.

If keys are lost, locks should be changed at once, or the vehicle exchanged with a similar one, kept at another location.

Vehicle and trailer records

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

- 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;
- Mileage.

A photograph should be taken of 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.

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

Secure vehicles

Vehicles may be secured by means of a range of additional security measures. The following should be considered.

- Using security equipment - it will make vehicles less attractive to criminals. Discussions on this should be held with insurers, including 'goods in transit' insurers, vehicle dealers, transport security consultants and security-equipment manufacturers.
- Having 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, considering the security equipment already fitted and what extras could be fitted.
- The 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 anti-theft 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. For instance the UK 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 vehicles are fitted with approved systems a company may qualify for reduced insurance premiums. 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 sets out the main types of security systems available for commercial vehicles and how manufacturers are improving vehicle security.

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.

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, the following should be taken into account:

- Vehicle type;
- Risk to both vehicle and load;
- Loading and unloading aspects.

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 hand brake; 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, consideration should be given on whether it needs to be:

- Manual (set by driver) or automatic (self-setting at all times) or
- 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. As a minimum there should be a 4-hour back up facility.

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.

Companies should follow the recommendations in standards e.g.

- Specification for theft prevention devices installed as original equipment;
- Code of practice for devices installed after vehicle marketing; and
- Code of practice for the protection of goods in transit.

Standards may also deal with the specification for vehicle cab locking systems and the security of the load bed areas.

Roof markings - high consequence dangerous goods

The wide use of roof markings on large goods vehicles helps airborne enforcement officers to identify stolen vehicles. Competent authorities may encourage carriers to use roof markings, particularly those carriers involved with High Consequence Dangerous Goods

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 the tractor unit as well as the trailer, tank or container. Where a single shared alarm system covers the tractor as well as 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 can be made of 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.

ANNEX IV

Company security plan template

When developing a security plan, every company should consider its own individual circumstances, and so may need to make reductions, variations or use something different. The following is only a suggested template and should not be taken as the only solution

Any parts of the following template that are not deemed appropriate or cannot be answered, should be deleted

It should be kept in mind that a security plan is subject to the provisions of in particular

- 1.10.3.2.2 (f): evaluation, testing and review of the plan
- 1.10.3.2.2 (g): ensure physical security of transport information contained in the plan.

ROAD TRANSPORT SECURITY PLAN

[insert name of company]

IMPLEMENTED – [insert date]

FOR USE INSIDE THE COMPANY ONLY

TABLE OF CONTENTS

SECTION 1: Company details

- **Name of the company**

  [Insert text]

- **Full Correspondence Address and contact details (telephone – email)**

  [Insert text]

- **Full address and contact details (telephone – email) of site to which this security plan applies**

  [Insert text]

- **Name and contact details (telephone – email) of nominated security co-ordinator**

  [Insert text]

- **Summary list of high consequence dangerous goods handled (e.g. in the format of Table 1.10.5)**

  [Insert text]

SECTION 2: Management of Security

A. PERSONNEL

- **List of people responsible for the management of security issues and their duties**

  See Annex A

- **List of people authorised to handle High Consequence Dangerous Goods**

  See Annex B

B. PROCEDURES (insert text or reference)

- **for recording meetings and actions with regard to security**
- **for receiving and disseminating security information to relevant staff**
- **for investigating security incidents**
- **for dealing with security alerts**
- **for the storage of security sensitive information (hard copy as well as electronic copy)**
- **for accounting for the movement of high consequence dangerous goods over the previous years**

  [Insert text]

C. SECURITY EQUIPMENT

- **Details of security equipment, including the maintenance programme and the actions to be taken in the event of an equipment failure**

  [Insert text]

D. SECURITY TRAINING

- **Details of security awareness training programme**

  [Insert text]

- **Details of specific security training programme for personnel with security duties**

  [Insert text]

- **Details of procedures for maintaining training records**

  [Insert text]

E. SECURITY TESTS

- **Details of plans and records of security drills and tests**

  [Insert text]

SECTION 3: Communication

A. COMMUNICATION LINKS BEWEEN SITE AND VEHICLES

- **Details of communication links with vehicles, including back-up links**

  [Insert text]

- **Details of communication links between site personnel with security duties, including back-up links**

  [Insert text]

B. SITE SECURITY ALERT

- **People to be informed in case of a site security alert (both inside as well as outside the company e.g. police)**

  [Insert text]

SECTION 4: Measures of Security

DESIGNATED AREAS WITH RESTRICTED ACCESS

- **List of designated restricted areas or buildings, mentioning in detail for each area or building:**
  - **the access points**
  - **indicating if members of the public are allowed access**
  - **security equipment to restrict and monitor access e.g. fencing, perimeter intruder detection systems, lighting, CCTV, etc**
  - **security procedures to restrict and monitor access e.g. patrols, pass system, identification of persons**

[Insert text]

VEHICLE PROTECTION

- **Details of equipment fitted to vehicles or procedures in place to better protect against theft or interference with that vehicle or its load**.

[Insert text]

SECTION 5: Any miscellaneous information

This section should be used if it is wished to provide any additional information felt to be relevant to the security of the site.

ANNEX A: List of people responsible for the management of security issues and their duties

NAME	POSITION	DUTIES

ANNEX B: List of people authorised to handle high consequence dangerous goods

ANNEX C: Restricted Area schematic

ANNEX D: <u>Record of when the Security Plan has been amended</u>

DATE AMENDED	AMENDMENT MADE