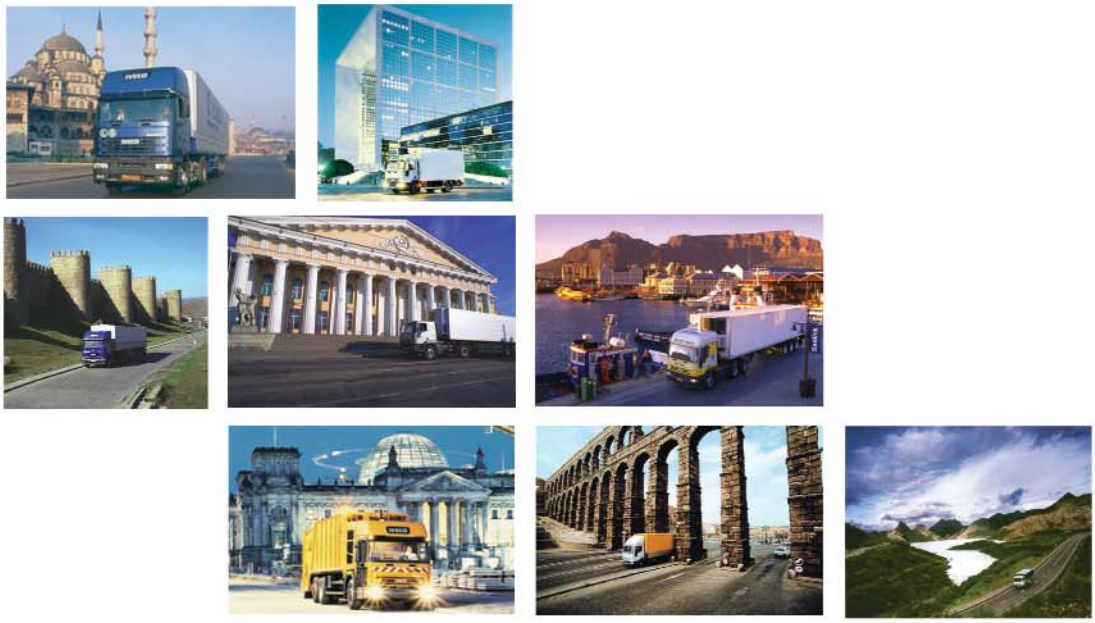
IRU Road Transport Security Guidelines

Voluntary Security Guidelines for Managers, Drivers, Shippers, Operators Carrying Dangerous Goods and Customs-Related Guidelines



International Road Transport Union

IRU Road Transport Security Guidelines

Voluntary Security Guidelines for Managers, Drivers, Shippers, Operators Carrying Dangerous Goods and Customs-Related Guidelines

Geneva 2005

Table of Contents

Preface

Following a decision taken by the IRU Goods Transport Council at the Yokohama meeting in April 2004, a Task Force on Security (TFS) was established with the objective to elaborate voluntary security guidelines for road transport operators.

Representatives of 10 IRU Member Associations expressed their wish to take part in the work of the TFS. Experts from 8 associations (AFTRI, ANTRAM, ATRH, DTL, FEBETRA, RHA, TLN and ZMPD) took an active part in the elaboration of the guidelines, launched in June 2004.
During the consultation phase, it was agreed that the final product of the TFS activities will be presented in the form of voluntary IRU Road Transport Security Guidelines, providing practical advice for:

- Managers,
- Drivers,
- Shippers,
- Operators carrying dangerous goods (elaborated by the IRU GEMD group), and,
- Customs-related guidelines.

The latter, were elaborated in close cooperation with the World Customs Organisation (WCO) and commented by the IRU Commission on Customs Affairs (CAD). In their final form, they represent a framework for voluntary cooperation between customs authorities and road transport operators and/or their representative associations.
The IRU Security Guidelines should be seen in combination and used together with other IRU security-related tools, such as the IRU-ECMT brochure on guarded parking sites in Europe, the brochure on control and enforcement bodies, the TIR checklists etc., most of which can be acceded on-line on the IRU website.

Although mainly inspired by concerns related to terrorist-related threats, these IRU voluntary guidelines represent an original combination of guidelines addressing both terrorist-related and conventional (theft of cargo and vehicles, attacks on drivers etc.) security.
The IRU Security Guidelines and the recommendations given are by definition general and deliberately detailed, so that all reasonably foreseeable cases and situations could be addressed. It is only logical that before recommending/applying them in specific circumstances or at national level, they should be adapted to meet the specific national situation, culture and legislation.
It was not possible to integrate all comments received. However, the commitment and richness of the input demonstrates the potential that exists within the road transport industry to further develop and improve its capacity to anticipate and react to both conventional and terrorist-related threats.

The IRU Security Guidelines are not only a technical instrument to raise awareness and assist road transport operators in taking appropriate practicable and proportionate preventive measures to minimise risk of theft or misuse of goods or vehicles for terrorist purposes, but it should also become a political instrument to demonstrate to society, politicians and partners in the public and private sectors the road transport industry's commitment and responsible behaviour.
It is only natural to put these voluntary guidelines to good use by making cooperative arrangements with national and other authorities, so that efforts and investments made by the road transport industry as a whole and by individual operators to improve security are rewarded both politically and through the market mechanism.

Best practices of jointly produced guidelines by industry and authorities, such as those existing in several European countries, should become a privileged tool to enhance public-private partnership.

Martin Marmy, IRU Secretary General

IRU Position: Haulage Security in the EU and beyond

This Position was adopted by the IRU Goods Transport Council at its meeting held in Yokohama, Japan, 21 April 2004.

Analysis

In the aftermath of 11 September 2001, much attention has been focused on improving security in transport and logistics. Initial measures focused on air and maritime transport; attention is now turning to the whole logistic and supply chain, which covers all modes of transport, including the road mode.

The IRU position is fully consistent with the European Union Economic and Social Committee on "Security of Transports" (Official Journal C 061, 14/03/2003 P. 0174 – 0183) striking the balance between Security and Facilitation:

> "If security procedures become too stringent the business of transporting goods could grind almost to a halt, which would give terrorists the success they were seeking.
>
> New security measures should be balanced in relation to the objectives they pursue, their costs and impact on traffic.
>
> Unilateral measures are unacceptable, especially when they are applied asymmetrically and to the detriment of the interests of third countries.
>
> Given the international character of … transport, security requirements should be based on reciprocal arrangements, uniformly applied and enforced without discrimination and must allow for the most efficient flow of trade."

Position

The haulage industry is fully conscious of the need to contribute to security in road transport. For clarity purposes, in this Position, the IRU limits its considerations to security against terrorism and conventional crime, mainly related to international border crossing transport operations, excluding "classical" aspects of road safety, even if safety and security matters are often interrelated. The safety aspects are dealt with by the industry under other headings.

Enhanced security is in the road transport sector's own interest. The role of States and their authorities in ensuring general security is however irreplaceable. It is their basic obligation. The goodwill and active participation of the road transport sector are essential to the success of any measures designed to improve security.

It should also be borne in mind that zero risk does not exist and total security can never be guaranteed.

1. **Competition in a globalised economy demands efficient logistic systems** whereby operators constantly strive to improve quality, safety and security without compromising efficiency and sustainability.

2. **Facilitation of transport and trade cannot be ignored**, even when security considerations are high on the agenda. It is essential to strike a proper balance between security and facilitation of formalities and procedures, in particular at frontiers.

3. Security concerns do not represent a **reason for modal shift**: the road transport sector does not represent a higher risk than other modes of transport.

4. **Security co-operation between the public and private sectors can be extremely effective** and should therefore be reinforced. The road transport industry cannot take over state functions.But it can shoulder its own responsibilities, for example in dangerous goods transport.

5. **Existing security/facilitation instruments** offering both security and facilitation benefits should be used to the maximum, such as the United Nations' TIR or the EU's Common/Community Transit systems.

6. **Fraud in customs transit systems** and people smuggling must be fought by customs authorities acting in a determined manner to identify the person(s) directly liable for the crime. Furthermore, legislation and self-regulation in customs transit management systems, protecting the rights of honest traders, introducing computerised systems to ensure rapid data exchange and tightening admission criteria to customs transit systems, should widely be implemented.

7. **"Self-security" measures** by the haulage industry should remain high on the agenda whereby the driver plays a crucial role, although all actors have their own responsibilities. In order to tackle these, the IRU will elaborate voluntary security guidelines for the haulage industry. Such efforts by the sector to improve security should be duly recognised.

8. **Duplication of effort by international bodies is harmful and must be avoided.** The road transport industry wishes to see an efficient harmonisation of all security related efforts on the international scene.

9. **Security policies must be information-based.** Rational and effective measures to enhance security can only be based on reliable information and understanding of international crime and terrorism as well as security-related risks and intelligence information.

10. **Security related financial burdens fall on the end users.** Legislators must keep in mind that financing security systems falls on the end users and beneficiaries of goods and services either as consumers or tax payers.

11. **Enhanced security should not reduce operators' freedom unnecessarily.** Transport infrastructure security must not lead to unwarranted restrictions on transport operators' easy access to roads, ports, terminals and other infrastructure facilities.

12. **"Authorised transport operators" should enjoy facilitation.** The road transport sector can accept, in principle, the introduction of the official designations such as "regulated agent","known shipper" and "authorised transport operator", on the condition that real facilitation benefits are granted to players so designated. Conditions for the granting of such a designation should be selected very carefully and implemented in a fair manner, to avoid any discrimination between hauliers. Haulage associations cannot be made responsible for the implementation of the "authorised transport operator" designation.

    Ideally, a unique designation should be granted for the territory of the whole EU. Member States should base the selection criteria for the "authorised transport operator" status on the conditions of access to existing customs transit systems (e.g. TIR Convention, Annex 9, Part II) or those of access to the haulage profession.

13. Electronic advance customs declarations should not be implemented hastily! Advance electronic customs declarations will require considerable changes to current practices and substantial investment. Adequate implementation time and suitable facilitation incentives should be provided while the possibility to use paper documents should be kept.

14. A 24-hour pre-arrival notification to customs authorities in case of border crossing traffic is excessive for road transport. Just-in-time requirements simply do not allow such a long pre-notification period. A two-hour limit for electronic pre-arrival/departure declarations or four-hour limit for hard-copy alternative seems to be more realistic.

15. The industry supports the use by customs of "single window" or "one-stop-shop" control technology and "risk management", as well as the use of a unique cargo identification number. The definition and input of this number through a "single window" into the logistic and supply chain should happen only once.

Chapter 1: Recommendations for Managers

These Security Guidelines contain recommended best practices, measures and procedures that ***managers of road haulage companies*** *may use to enhance conventional and terrorism-related security in their companies.*

The objective is to raise security awareness and assist road transport operators in implementing preventive measures to minimise risk of theft or misuse of goods or vehicles for terrorist purposes.

Road transport operators and in particular those:

- *transporting high consequence dangerous goods, chemicals, drugs, foodstuffs, cars and other goods that, because of their nature or value, may be particularly exposed to terrorist or criminal threat,*
- *involved in operations in security-sensitive environments*
- *driving on vulnerable routes*
- *driving to or from security-sensitive places*
- *dealing with high-profile companies that may be particularly exposed to security-related threats*

are invited to make use of the appropriate part(s) of recommendations below, according to the size of the company, its risk exposure and its place in the supply chain.

1. Company policy

1.1. Use security guidelines, in particular, nationally agreed security guidelines elaborated by your trade association, authorities, insurers and manufacturers.

1.2. If feasible and appropriate for your company, appoint a (senior) member of staff in charge of security issues. If this not be possible, the company manager should be in charge.

1.3. If appropriate, carry out a company-specific risk assessment (model Operational Review annexed) and integrate security management in the overall management of the company.

1.4. Issue a Security Policy Statement/Instructions setting down general principles for secure operations and include this in the company and driver's manual/handbook.

1.5. If appropriate for your company, establish a Security Plan (model annexed) and/or a check list of basic security rules and procedures for your staff (separate guidelines for drivers avail able). The security plan could contain specific allocation of responsibilities, the risks concerned, the measures to be taken in the event of a security incident and the review of operation and assessment. Specific attention should be paid to vulnerable areas and times, such as halts, nights, etc.

1.6. Regularly re-evaluate security-related assessments/reviews, plans and checklists, including, when feasible, via external or internal auditing.

1.7. Draw your staff's attention to security issues (i.e. via in-house notice boards) and stimulate awareness among management.

1.8. Pay special attention to sub-contractors and self-employed contractors and their staff/employees/workers, in particular when they are employed in key positions/operations.

1.9. Establish a general and operational link with local (police) authorities and alert them regarding security-related incidents.

2. Procedures and Staff

2.1. Documentation and information

2.1.1. Keep documentation in a secure place. Safeguard computer access and information in documentation/computer areas and control/monitor access to information systems and use of information. Back up information regularly.

2.1.2. If appropriate, fix times for preparing documentation and use special procedures to pre pare last minute or emergency shipments. Consider the introduction of signatures for all process checkpoints (document preparation, sealing, truck inspection, delivery etc.).

2.1.3. Keep records of your security-related activities.

2.1.4. Ensure that details of your vehicles, trailers and loads are available quickly. The minimum information available should include: vehicle registration number, trailer serial number, make, model, body type, vehicle identification number, engine number, gear box number, livery details, number of axles, special equipment fitted with serial numbers, security devices fitted and mileage.

2.1.5. Consider having similar information on loads - type, sensitivity, quantity, packing, labelling, loading method, fixing, etc. – readily available.

2.1.6. In case of high-value or highly security-sensitive goods, limit the information related to these goods in commercial documentation on board the vehicle to the minimum necessary. Make sure that this kind of information is dealt with by trustworthy persons.

2.2. Recruitment

2.2.1. When hiring new staff members, check candidates' identity (original identity card/pass port), references (insurance, criminal convictions, previous employers and not only the last one) and, in addition for drivers, the validity of their driver's licence, when possible and when allowed by national legislation. Check all drivers' licences regularly, e.g. at six-month intervals.

2.2.2. Some general recruitment rules are: Include security elements in the recruitment interview. Check identity cards, driving licences and other similar documents for alterations. Keep copies on file. When checking references, use independent sources as much as possible (try to speak to previous employers) and original documents (i.e. birth certificate). Do not accept open references, such as "TO WHOM IT MAY CONCERN". Try to obtain confirmation of employment history (i.e. five to ten years) in writing. Ask for at least two character references. Referees should have known the candidate for a sufficiently long time.

2.2.3. Work with partners and staff recruiting interim companies that have proven good repute, i.e. are well-known, are members of a recognised professional organisation or are bound by professional standards.

2.2.4. Incorporate security duties and obligations into the employment contract. Contracts should make clear that employees/drivers will face disciplinary action if they fail to carry out these duties. Security responsibilities should also feature in employees' job descriptions.

2.2.5. Take documented action where employees fail to comply with company security policy.

2.3. Training

2.3.1. Regularly organise security training and refresher course covering behaviour, vehicles and premises. Security should become a daily routine for your employees and management.

2.3.2. Security awareness training should cover 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 breach of security. It should also include awareness of security plans (if appropriate) commensurate with the specific responsibility of the individuals and their part in implementing any security plan.

2.3.3. When available, provide a Driver Security Manual/Handbook or Security Checklist.

2.3.4. Regularly check that employees/drivers understand and use security equipment in vehi cles and premises.

2.3.5. If feasible, invite external experts from competent authorities, such as police, customs etc., and other relevant external bodies to train/instruct/inform your staff.

2.4. Prevention and instructions

2.4.1. Give clear and precise instructions. Document them and, if need be, distribute written instructions. Check that these are understood, accepted and complied with by all staff.

2.4.2. New staff members should be properly instructed and trained.

2.4.3. Drivers should receive specific security instructions each time they drive on the road (see driver's guidelines).

2.4.4. Ensure drivers are issued with appropriate security equipment.

2.4.5. Establish a standard reporting form and encourage personnel to report incidents, even minor ones.

2.4.6. Analyse incident reports at regular intervals and, if need be, adapt company strategy accordingly.

2.4.7. Be alert to changes in employees' behaviour that may indicate a potential conflict of interest.

3. Vehicles

3.1. Install security equipment in accordance with the type of cargo carried, the itinerary and other specific features of the security environment and the transport operation. Make sure that equipment is switched on when appropriate.

3.2. Security equipment should be checked regularly, including by the installer.

3.3. All vehicles should have extra means of immobilisation. When purchasing vehicles, give preference to in-built security equipment and consider purchasing additional security devices.

3.4. Where appropriate, use security seals to protect the load.

3.5. To the extent possible, restrict cargo-specific information on the tarpaulin and the body of the vehicles (anonymity is recommended).

4. Communications

4.1. If appropriate and affordable, use modern communications systems, such as vehicle tracking systems, SOS messaging etc., to detect any unexpected behaviour of the vehicle in real time.

4.2. Establish routine communication procedures between vehicles and company head office.

4.3. When a driver is sent to a customer to load/unload for the first time, send advance information to the customer identifying both the driver and vehicle.

4.4. Where available, supply drivers with emergency telephone numbers or other appropriate phone numbers to enable them to liaise with the company and/or the relevant authorities and, if abroad, embassies and, to the extent feasible, road transport associations in the countries “en route”. Instruct them always to call the company first.

5. Premises and sites

5.1. According to your company specific risk assessment, define protection perimeters, visitor and personnel access, as well as parking zones.

5.2. Make sure that you have an effective system to prevent unauthorised entry and that it is operated properly.

5.3. When affordable and depending on risk assessment, install security and surveillance equiement (gratings, lighting, alarms, cameras, guards).

5.4. Limit access to security and surveillance equipment.

5.5. Establish a system for monitoring people entering and leaving your site(s).

5.6. Regularly inspect on-site installations, access areas, parking areas, remote parking areas, loading bays, key storage and other storage areas.

5.7. Keep all vehicle/premises keys in secure places. Define secure practices to monitor move ment and storage of such keys.

5.8. Storage, issue and return of staff uniforms should be monitored.

5.9. Report any complaint (theft, aggression etc.) to the police.

6. Transport operations

6.1. Instruct drivers and, if need be, provide written en-route instructions (checklists, driver’s security guidelines etc.).

6.2. Identify guarded parking areas. Plan all halts, breaks and overnight stops in advance. In the event of an unscheduled halt, instruct drivers to keep all doors locked, even when talking to people, in particular when transporting vulnerable loads.

6.3. When possible, vary routes and drivers.

6.4. Instruct driver to keep keys on his/her person at all times and not to leave them where they might be copied. Make sure that keys are not vehicle-identifiable, i.e. that there are no obvious vehicle details written on the key ring. He should not leave the vehicle until he has ensured that it is fully locked, secure and security equipment switched on.

6.5. Instruct drivers not to give lifts or have unauthorised people on board, also bearing in mind conditions laid down in insurance contracts.

6.6. Encourage drivers to report anything unusual (any irregularity in loading, locking, sealing, documents, changes in delivery instructions, suspicious delays, people or vehicles, destination, etc.) to your company or, in emergency, to the police.

6.7. Brief drivers on how to behave in the event of hijack or criminal attack, whilst putting their own security first.

7. List of useful security-related addresses to contact (country-specific):

7.1. Trade association.

7.2. Other relevant trade associations (partners from related industries, i.e. shippers, chemical, food etc.) and/or insurers.

7.3. Relevant authorities (Ministry of Transport, Police, Anti-Terrorist Hot Line, etc.).

7.4. National emergency call numbers.

7.5. Specialised security management companies with whom the transport company may have a contract.

7.6. Other.

8. Elements for a Voluntary Company Security Plan

The Security Plan could be elaborated in three stages. During the first stage, threats are identified (i.e. current security climate, information from local police and/or other relevant bodies/authorities, specific details concerning your company or its partners/customers that may attract a terrorist or criminal attack, your company location, general situation in foreign countries visited). During the second stage, the specific vulnerabilities to be addressed are identified. The third stage is the identification of security measures to reduce risk to accept able levels.

8.1. Person responsible

The road transport operator appoints a competent, qualified employee or a person, with whom contractual relation exists, to be responsible for security.

His/her main duties are: conducting a risk assessment, identification and implementation of defensive measures; devising and maintaining security plans and emergency (evacuation and re-occupation) plans; liaising with police, emergency services and other relevant authorities and partners; arranging staff training, communications and drills.

The appointed person must pass on all suggestions and information from employees regarding security to the management. The person must be allowed to act on his/her own initiative to reduce immediate security and should be responsible for providing adequate information on security matters to employees.

8.2. Records

The road transport operator must keep records of security-related activities, transport operations and security-sensitive goods transported. The records may need to be made available to enforcement authorities and other public bodies involved in security risk prevention.

8.3. Operation review

When establishing the Security Plan, all operations for the storage, handling and distribution of security-sensitive goods as well as any vulnerability assessment must be reviewed by the management. At least once a year, a general security review of operations must be carried out jointly by management and the person in charge of security. Road transport operators must demand preventive security information from their partners, customers and suppliers.

8.4. Staff

Security measures (training, operational practices, equipment and resources) should be com municated clearly to employees. Every employee with activities related to security-sensitive goods or transports must receive special training and/or instructions. When they take up functions related to security-sensitive goods and/or transport operations, such employees must also receive clear information from the management about specific security measures to be adopted.

8.5. Reporting of risks or incidents and crisis management

Every employee with activities related to security-sensitive goods or transport operations is obliged to report to the management and/or the person in charge of security about any threat observed or any incident affecting security. The management and/or the person in charge of security will decide if the authorities should be informed.

To manage emergency situations, operators should prepare emergency plan(s), a crisis management team, train in-house emergency response personnel and establish emergency coordination procedures.

8.6. Evaluation

Security evaluation and testing procedures should be established, as well as periodic reviews and updates.

8.7. Confidentiality

Security of information and documentation should be guaranteed. All employees with activities related to security-sensitive goods or transport operations should be instructed not to inform other persons about itineraries and the types of goods transported and handled by the company and its customers, except if such information is needed according to other regulations (e.g. information on transport and customs documents) or demanded by authorities. Information on security measures in place and the contents of the security plan must be kept confidential.

8.8. Additional security measures

In addition to the measures described above, road transport operators should analyse whether the infrastructure and operations organised by the company or its customers require additional security measures.
The security plan should also address personnel security, unauthorised access and en route security.

8.9. Cooperation

Transport operators cooperate with their partners in the transport chain and with the authorities to exchange information on threats, apply appropriate security measures and respond to security incidents.

9. Voluntary Guidelines for a Company Operational Review

Stage 1

Make a statement of overall security needs and involve all stakeholders to discuss, agree upon and accept solutions along the following lines:

9.1. Company policy
State main items related to company profile (size, operations, staff, fleet), risk exposure and company security policy.

9.2. Site or building
State the location and purpose of the site/building and any background comments on its priority or importance. State its boundaries in order to ensure that it is clear which land can be used for security measures.

9.3. Transport operations
List destinations and types of transport. Include en-route infrastructure, in particular relating to vulnerable areas (e.g. halts) and time frames (e.g. night). Consider risks related to taking goods in charge and delivering them.

9.4. Stakeholders
List all stakeholders who should have an interest in the operational security of the site/build ing. Confirm whose priorities might be most important and how any conflicting priorities might be resolved.

9.5. Assets to be protected
List the assets that are to be protected (human, physical, intellectual) together with their value (human, financial, operational and political).

9.6. The threat
State the perceived threat(s), the likely abilities of attackers, the tools they may be expected to use, and the most likely methods of attack. Try to estimate in broad terms the probability and frequency of attacks occurring.

9.7. Consequences of not implementing measures
State what these are in terms of physical, financial, operational, morale and political embarrassments/consequences.

9.8. Areas of concern and vulnerabilities
Areas which are particularly vulnerable should be identified.

9.9. Success criteria
Which developments would indicate that security measures have been successful.

9.10. Other factors
Include any constraints, such as planning permission, neighbouring facilities, staffing levels, response forces and environmental considerations (weather and vegetation). This section may state which possible solutions are more appropriate and why.

9.11. Possible solutions
When considering the areas of concern and vulnerabilities, various possible solutions may come to mind. These thoughts should be noted together with any constraints that may apply.

Stage 2

Detailed review of each area of major concern, as identified under stage 1, with possible outcome and performance specifications.

Such specific areas may include company and staff aspects, en-route infrastructure, security fencing, lighting, surveillance systems, detection systems, physical delay systems, access control, etc. Depending on the complexity of the issue, an outside security consultant may be used to prepare these.

10. Emergency Reporting and Model of simplified Incident Report

Should you have a security incident or suspicion regarding a possible security situation, you must notify your local police station and/or the anti-terrorist units (hot line).

10.1 Key steps in the immediate aftermath of a security incident include:

10.1.1 Confirm exact location and date/time vehicle/load last seen,
10.1.2 Obtain details of vehicle/load,
10.1.3 Report details of vehicle/load to police and note Police Incident Number you are given,
10.1.4 Report details to insurer and keep copies of claims submitted.
10.1.5 Additional steps may include: inform other drivers and companies about stolen vehicle/load, as well as specialised agencies/companies dealing with stolen vehicle/cargo.

10.2 Main elements of a security incident report may cover:

10.2.1 Vehicle identification
10.2.2 Date and location of occurrence, including topography (bridge, tunnel, crossing, etc.)
10.2.3 Particular weather, if appropriate
10.2.4 Description of occurrence
10.2.5 Type of vehicle and goods involved
10.2.6 Cause(s) of occurrence
10.2.7 Consequence(s) (for persons, load, damages, involvement of authorities)

Chapter 2: Recommendations for Drivers

*These Security Guidelines contain recommended best practices that **drivers of road haulage companies** may use to enhance conventional and terrorism-related security in their companies.*

The objective is to raise drivers' awareness and improve security whilst suggesting appropriate preventive measures to minimise risk of theft or misuse of goods or vehicles for terrorist purposes.

1. Remember

1.1. Your truck is your livelihood. Apply employer's security rules – they are designed to guarantee security and protect yourself, your fellow citizens, the load and the vehicle.

1.2. The tips in this fact-sheet will help you to stop truck thieves and prevent misuse of goods or vehicles by criminals and terrorists.

1.3. Please take the time to read this leaflet and discuss any questions you may have with your employer. Keep this safe in your cabin for future reference.

2. Respect company security policy and advice

2.1. Always follow this advice. If you fail to do so, your employer could take disciplinary or legal action against you .

2.2. If you witness suspicious or criminal behaviour, call the police, immediately.

2.3. Always keep your employer informed of any untoward event.

3. Plan ahead

3.1. Plan details of your route beforehand in accordance with the instructions given to you by your employer and/or his representative. This will avoid having to stop to ask for directions. If you know exactly where you are going, no-one can mislead you with wrong directions. Never follow directions given to you by unknown persons, e.g. present at delivery addresses – check first with your employer.

3.2. Avoid unnecessary vehicle immobilisation.

3.3. Avoid routine stops for cigarettes, newspapers etc., by buying them before beginning the journey.

3.4. Refuel only at known safe locations and, where possible, onsite before beginning the journey.

3.5. Check that all security devices are working.

4. Taking charge of goods

4.1. Whenever possible, watch out for incorrect or short loading by careless or dishonest warehouse staff.

4.2. Check that the load matches the collection note. If applicable, take note of the seal number.

4.3. Report any irregularity in loading, locking or sealing.

4.4. Make sure it is clear where you will deliver and who will receive the goods.

4.5. Get a contact telephone number, if possible.

4.6. Note down any discrepancies, in accordance with your employer's instructions.

4.7. Be discreet about your load and its destination.

4.8. Make sure your cabin and the load compartment are secure.

4.9. When loading or unloading, lock the cabin. Do not leave transport documents and/or personal belongings visible in the cabin.

5. Delivering goods

5.1. Check the load seal is still intact and the number is the same as on the delivery note.

5.2. Check that quantities and, if possible, weights match the collection and delivery notes.

5.3. Make sure you are delivering to the right place (check collection and delivery against the notes).

5.4. If the delivery instructions are changed, get written confirmation of the changes from senior staff at the delivery address or from your employer. Should you need additional information "en route", do not follow directions from unknown persons - check with your employer first.

5.5. Make sure that there is a clear signature and printed name on the proof of delivery note.

5.6. If possible, supervise unloading operations personally.

6. Be secure and safe during transport and parking

6.1. Confidentiality and precautions

6.1.1. Avoid talking about loads, their value, itinerary, loading/unloading and delivery locations to anyone, including other drivers, even by telephone.

6.1.2. Avoid taking on board any person who is not a company employee. Never give lifts.

6.1.3. Never leave personal belongings on view.

6.1.4. Avoid regular routes or stops - a recognisable pattern makes you an easier target for thieves/criminals.

6.2. Keys and locks

6.2.1. NEVER leave keys in or on your truck.

6.2.2. When you leave your vehicle, always lock it and always take your keys with you. Never leave them in the cab. Remove ignition keys even when going to pay for fuel or when making a delivery.

6.2.3. Make sure keys cannot be identified - don't leave anything on the key ring that reveals who they belong to or what vehicle they fit. Never leave them where strangers can see them; and always keep them somewhere safe.

6.2.4. If you store your keys at your company's operating base, make sure they are in a lockable place out of sight of strangers. Never use a "hiding place", for example, inside the front bumper.

6.2.5. Keep the load compartment locked even during driving.

6.3. Prevention

6.3.1. Make sure you understand and use the vehicle's security equipment and check if it's working properly.

6.3.2. Carry out visual checks of the vehicle at every halt: check the load and seals (are they intact?)

6.3.3. In case of an unscheduled stop, keep doors locked. Do not leave the cabin without making sure that it is fully locked and secure, with the alarm switched on.

6.3.4. Whenever possible, get a colleague to watch your vehicle while you eat.

6.4. Parking

6.4.1. Do not park in isolated areas.

6.4.2. Whenever possible, decide where you are going to park overnight before starting your journey. In case of a change, inform your company about your new location.

6.4.3. Do not make a habit of using insecure casual parking areas.

6.4.4. Try to park your vehicle within sight while you eat.

6.4.5. Park with the loading doors close to another vehicle, building or wall.

6.4.6. Never leave windows open when away from vehicle.

6.4.7. Upon return to your vehicle, check all around for signs of interference, including the load security seals.

6.5. Reporting and forced stops

6.5.1. Report back to your employer, in accordance with employer's instructions.

6.5.2. Be cautious if you are forced to stop, for example, at the scene of an accident or an emer gency, or at police stops. Closed roads "en route", with or without an indication of an alternative itinerary, should be reported to the company.

6.5.3. During security alerts, follow the advice given to you by local police. Make sure someone stays with your lorry if you have to leave it. If you are alone, leave a clearly displayed note explaining where you are, how you can be contacted and when you will be coming back to your truck.

7. What to do in emergency situations, theft or acts of aggression

7.1. In the event of an abnormal situation or theft of load

7.1.1. If the tarpaulin or rear doors are open, check the load.

7.1.2. In case of theft, try to evaluate losses.

7.1.3. Immediately inform your employer and the police.

7.2. When the vehicle has been taken

7.2.1. Inform your employer: if the vehicle is equipped with a tracking device, the employer will take the necessary measures.

7.2.2. Inform the police and make an official declaration of theft.

7.3. In cases of aggression (or during theft in progress)

7.3.1. Don't resist/oppose the perpetrators.

7.3.2. After the incident, inform the police as quickly as possible either using a roadside telephone (your location can be identified exactly) or from another phone or mobile phone (in this case, indicate your exact location) or by CB radio.

7.3.3. Inform the employer.

7.3.4. File an official complaint with the police.

7.4. In addition

7.4.1. If your truck or trailer has a roof marking and you are the victim of a crime, make sure you tell the police.

7.4.2. Report in confidence any information about criminal activity.

8. Protect yourself

8.1. Security comes first. Be cautious and firm in your decisions.

8.2. Hide personal property from view.

8.3. Make sure you have adequate (company) insurance cover.

9. Useful telephone numbers and addresses (where appropriate)

9.1. Emergency numbers (if possible in all relevant countries):

- Police …
- Anti-terrorist unit …
- Emergency situation …
- Fire-brigade …
- Emergency help …
- Specialised security management companies with whom the transport company may have a contract…

9.2. National stolen truck/load desk …

9.3. Crime stoppers …

9.4. Embassy (if abroad) …

9.5. Other ….

I have received and understood the above instructions from my company. I understand that if I fail to respect them I could be subject to disciplinary action by my employer .

Driver: …….....(signature) Date and time: ….....

Chapter 3: Recommendations for shippers/consignors

*These Security Guidelines contain recommended best practices that **shippers/consignors and road haulage companies** may want to use to improve security cooperation with other parties and enhance conventional and terrorism-related security in their companies.*

The objective is to raise security awareness and suggest preventive measures to minimise risk of theft or misuse of goods or vehicles for terrorist purposes.

Terrorism, theft and crime against the road transport sector have significant economic and social consequences. All actors in the transport chain - shippers, freight forwarders, logistics service providers, transport operators, customers, but also automotive manufacturers, insurance companies and public authorities - are involved in the fight against crime.

1. Personnel and site management

1.1. Carefully select personnel in charge of despatching goods. Thoroughly check their trustworthiness/reputation.

1.2. Establish a site management system covering identification, evaluation and management of security risks to people and information involved in despatching goods.

1.3. Limit access to loading areas and, if possible, provide several loading zones, each isolated from the others, and from the rest of the company premises.

1.4. Carry out a detailed audit of company internal procedures, especially for threat/theft prevention.

2. Training/Instructions

2.1. Instruct and where necessary train despatch personnel to manage security and theft risk.

2.2. Coordinate security-related instructions with your transport provider. Advise on the use of appropriate vehicles.

3. Risk and theft prevention

3.1. Optimum confidentiality of all out-going information

3.1.1. Protect information and data on consignments.

3.1.2. Limit explicit information on the type of cargo and its itinerary.

3.2. Means of transport

3.2.1. Verify vehicle characteristics: these should be adapted to the type of cargo transported, fitted with anti-theft devices, etc.

3.2.2. Verify vehicle quality: these should be equipped with chassis locking system.

3.2.3. It is preferable to refuse vehicles not conforming to agreed prescriptions.

3.3. Advance information to transport provider to avoid waiting times

3.3.1. Provide loading area opening hours.

3.3.2. Provide time-tables/loading rates.

3.3.3. Pay attention to waiting at borders and related risks. Whenever possible, provide relevant information to operators and alternative roads.

4. Transport organisational procedures

4.1. Service providers

4.1.1. Only offer loads to appropriately identified carriers.

4.1.2. Shippers should liaise with the Consignee.

4.1.3. Request in advance driver identity information for drivers loading/unloading for the first time at shipper's/consignor's premises.

4.2. Managing sub-contracting

4.2.1. Limit non-agreed sub-contracting and the number of sub-contractors within a single transport operation.

4.2.2. Monitor the whole transport operation and try to avoid load breaks/empty runs.

4.2.3. Only use transport operators of demonstrated good repute.

4.2.4. Demand report upon delivery.

4.2.5. Ensure that the various actors in the transport chain conform to contract specifications.

4.3. Loading

4.3.1. Ensure the actual presence of the shipper/consignor's representative during loading.

4.3.2. Try to make full loads; group loads where possible.

4.3.3. To the extent possible, avoid loading on a Friday afternoon for a Monday morning departure. In such cases, load goods preferably on the Sunday afternoon.

4.4. Securing the load (seals, packaging, product deactivation)

4.4.1. Packaging should be solid and adapted to the type of cargo.

4.4.2. Labelling should be as common and as ordinary as possible for the whole load (whether of little or great value). Make use of opaque film for the whole load. Regularly change external load appearance, approximately every fortnight (colours, codes).

4.4.3. Seals should be placed by the shipper at departure, in the presence of the driver - never by the driver. Include the seal number in the transport documents and have the consignment note co-signed by both the shipper and the driver. Verify that seals, the load unit and packaging have not been interfered with at each load break. Companies should change their seals every three months - shape, colour - to prevent counterfeit seals being made.

4.4.4. Define special procedures for high value/vulnerable cargos, i.e. communication between the vehicle and the company. If feasible, electronic disabling equipment should be provided and cargo should be shipped in separate part consignments.

4.5. Journeys

4.5.1. Consult/advise the transport operators on the planned itinerary in advance. Check halts and parking times.

4.5.2. Limit stops/parking times in agreement with the transport operator and according to current legislation.

4.5.3. Try to forecast in advance particular risk situations that may occur. The road transport operator should be informed about the value/vulnerability of the load, without necessarily informing the driving personnel of the precise type of cargo concerned. Establish stricter rules for transport operations which require a higher degree of surveillance.

4.5.4. Define itineraries in function of the confidentiality/vulnerability of goods and security environment. Consider border-crossing points, parking areas, ports of embarkation, railway stations in case of combined transport, terminals, etc.

4.6. Delivery

4.6.1. The destination address must be exact, transport documentation accurate and communication with transport clear and reliable.

4.6.2. Unloading areas should be accessible with clear signposting to the site.

4.6.3. Avoid waiting times outside normal working hours. Clearly specify these opening hours and organise transport in cooperation with the transport operator within the framework of company opening/operational hours.

4.6.4. Unloading should be swift and the number of employees available should be adapted according to the type of goods being handled.

5. Transport and insurance documents

5.1. Documentation

5.1.1. Only carry the strictly required number of copies.

5.1.2. Make the nomenclature neutral (remove special marks, references, codes - anything that enables the recognition of goods).

5.1.3. Apply/use seal number.

5.2. Insurance

5.2.1. It is recommended (optional) to insure goods beyond the standard level of liability reim bursement.

5.2.2. It is recommended to the company to take out insurance for the goods dispatcher

5.2.3. Provide a correct declaration of value, especially for high value/vulnerable goods.

6. Order specifications

6.1. Compile operational specifications - for the transport operator or the intermediary - that are as accurate as possible, including driving hours, delivery times, other timings to be respected, other service quality criteria, risk and theft prevention and including loading/unloading conditions, integrating specific security instructions.

6.2. When selecting transport operators, consider criteria such as good repute.

7. Information and cooperation in emergency/theft

7.1. Share information and experience in preventive security measures with your regular transport providers.

7.2. Inform your transport providers of any threats that may affect the transport operation.

7.3. Declare theft as soon as possible.

7.4. Give the driver or at least the transport operator a unique contact telephone number for cases of emergency or theft.

7.5. When a road accident affects the delivery of the goods, the transport operator should inform the consignee accordingly.

Chapter 4: Guidance for transporting dangerous goods by road

Introduction

International terrorism is not new and regrettably many countries experience it. But 11 September 2001 changed some of the assumptions on the degree of moral restraint shown by terrorists and their desire for self-protection and escape.

Therefore, governments must review how they plan to respond to terrorist acts, and associations such as the IRU and its Members have to assume their share of responsibility for the problem and encourage a culture of security awareness.

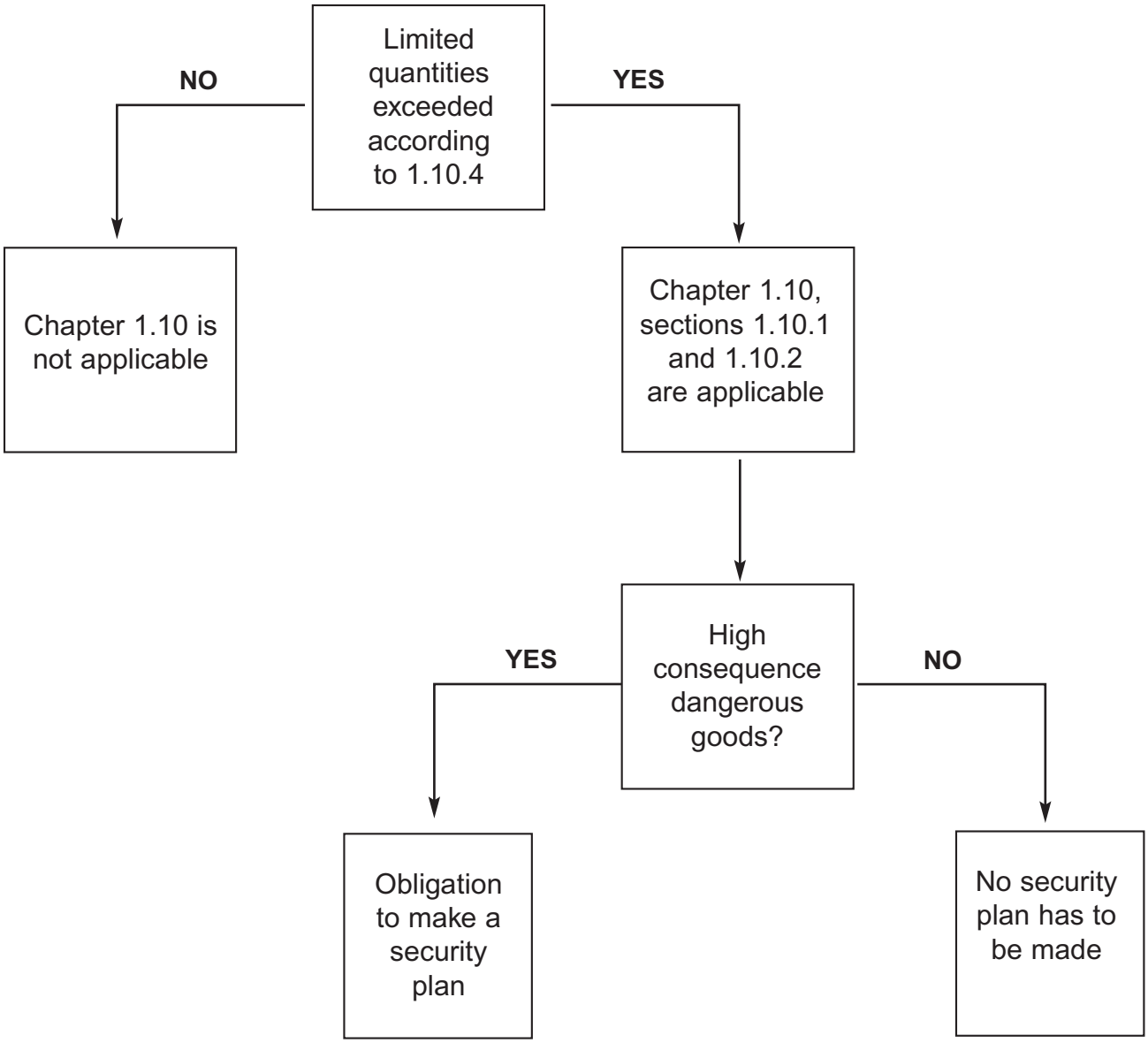
Security precautions cannot, of course, guarantee the prevention of future terrorist atrocities but it makes sound economic as well as social sense to identify and pursue effective and proportionate security precautions, which substantially reduce risks.

***Security measures** for the transport of dangerous goods by road, rail and inland waterways have been listed in a **new chapter of the ADR Agreement; Chapter 1.10.** The new provisions will enter **into force on 1 January 2005** with a transition period of six months.*

The transport companies concerned should not rely on these dates but start preparation and implementation as soon as possible. Security measures should be an integral part of the safety and quality management system of every company involved in the transport of dangerous goods. The purpose of this guidance is to assist small and medium-sized transport companies with the implementation of the new legislative security measures.

Security precautions come at a cost but the impact of terrorism should also be borne in mind. The question of who should bear the costs of improving security is easily answered: "all of us". As consumers, we are all customers of global distribution networks, of dangerous goods or any other commodity. Any extra costs added to the supply chain will ultimately be passed on to consumers through increased prices.

Flowchart


Limited quantities exceeded according to 1.10.4
NO
YES
Chapter 1.10 is not applicable
Chapter 1.10, sections 1.10.1 and 1.10.2 are applicable
High consequence dangerous goods?
YES
NO
Obligation to make a security plan
No security plan has to be made

1. Legal Base

ADR agreement	Chapter 1.10 - Security provisions Description of **"security"**: security, for the purpose of this chapter, refers to the measures and precautions taken to minimise the risk of theft or abuse of dangerous goods through which persons or the environment might be endangered.

2. General Provisions

Persons involved (1.10.1.1)	The haulier, driver, planner, (…) according to their responsibilities from the moment the transport order is accepted until the delivery of the goods.
Identification of the carriers (1.10.1.2)	No particular actions are required for an existing regular business relationship.When starting up a new business relationship, a written confirmation of at least the following elements is required: • Name and address of the haulier • Phone number of the haulier
Securing of areas (1.10.1.3)	Vehicles carrying dangerous goods have to be parked safely when not driving, in supervised or secure areas. Wherever possible, they should not be accessible to the general public. If such facilities are not available, the vehicle should at least be parked in: (a) A vehicle park supervised by an attendant who has been notified of the nature of the load and the whereabouts of the driver; or (b) A public or private vehicle park where the vehicle is not likely to suffer damage from other vehicles; or (c) A suitable open space separated from the public highway and from dwellings, where the public does not normally pass or gather together. These parking rules are not new and are taken over from chapter 8.4 ADR!
Identification of the crew (1.10.1.4)	• A driver's license or an identity card, including a photo graph, delivered by the competent authority is mandatory for each crew member. • Passengers are not allowed on board unless their presence is properly announced.

3. Security Training

Security awareness (1.10.2.1 and 1.10.2.2)	Training should not only be focussed on regulatory changes, but also address awareness of the nature of security risks, methods to reduce such risks, as well as an action plan in the event of a breach of security.

4. Security plan for listed high consequence dangerous goods (see 6)

Security plan (1.10.3.2.1)	All parties involved shall adopt, implement and comply with a security plan.
Minimum requirements of the security plan (1.10.3.2.2)	• Organisation chart mentioning the (internal or external) person(s) in charge of security, as well as his (their) specific competences in this field. The safety adviser may assume this function. • Paper or electronic records on the transport of dangerous goods should be kept for 5 years. The records should be classified in an orderly way (e.g. chronological). CMR notes may be used for this purpose. • Transport risk assessment, including routing systems, should be set-up and reviewed yearly by management; • Overview of preventive security measures related to personnel recruitment, training, planning and equipment to reduce risks. For example: - supply of a certificate of good behaviour, delivered by the com petent authority, before recruiting an ADR driver, if such a certificate is issued nationally, - pre-loaded vehicles should be left in a secure location, locked with alarms/immobilisers set and keys kept in a secure location; • Effective and up-to-date reporting procedures. Drivers should be clearly briefed on key steps to be taken upon discovering the theft of a vehicle and/or its load, with at least the obligation to immediately notify the local police force; • Evaluation of security procedures and periodic checks; security measures must be followed and updated to reflect changes in buildings and personnel and ensure they remain accurate and workable (e.g. fences, site access and its control, intruder-detection, etc.). • Ensure that the security plan is kept confidential and is not accessible to persons who are not directly involved; • Confidentiality clause for those employees whose activities are related to dangerous goods transport operations.
Tracking system (1.10.3.3)	The vehicle must be traceable during transport. A fitted mobile phone with fixed numbers may be considered as a valid tracking method.

5. Exemptions

Non-application (1.10.4)	All the above-mentioned requirements do not apply when the dangerous goods are carried in packages, in tanks or in bulk, in limited quantities (meaning not exceeding the quantities referred to in 1.1.6.3 ADR).

1. High consequence dangerous goods/quantities (ADR 1.10.5)

Class	Division	Substance or article	Quantity		
			Tank (l)	Bulk (kg)	Packages (kg)
1	1.1 1.2 1.3 1.5	Explosives Explosives Compatibility group C explosives Explosives	a a a 0	a a a a	0 0 0 0
2		Flammable gases (classification codes including only the letter F) Toxic gases (classification codes including letters T, TF, TC, TO, TFC or TOC) excluding aerosols	3000 0	a a	b 0
3		Flammable liquids of packing groups I and II Desensitised explosives	3000 a	a a	b 0
4.1		Desensitised explosives	a	a	0
4.2		Packing group I substances	3000	a	b
4.3		Packing group I substances	3000	a	b
5.1		Oxidising liquids of packing group I Perchlorates, ammonium nitrate and ammonium nitrate fertilisers	3000 3000	a 3000	b 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 A1 (special form) or 3000 A2, asapplicable, 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.**

Chapter 5: Framework for voluntary co-operative arrangements with Customs

Foreword[1]

Almost everywhere in the world, the road transport industry (haulage) is characterised by the existence of a great number of small companies. This highly fragmented industry is represented, on the national level, by road transport associations and, at international level, by the International Road Transport Union (IRU).

The IRU helped develop the World Customs Organisation's (WCO) model guidelines for increasing security in the supply chain. In the present document, these model guidelines have been reviewed and customised to reflect the specificities of the road transport sector.

1. Introduction

Terrorist atrocities around the world have drawn increased attention to the international dimension of terrorism and the possibility of systems involved in the international movement of people and goods being used for terrorist ends.

Equally, criminals have used legitimate trade as a cover for other illicit activities, such as illegal migration, drug trafficking, money laundering, customs and transit fraud, the movement of counterfeit goods and other offences which threaten the well-being of national societies and the international community.

Security Management is an integral part of an organisation's overall management system. The structure, responsibilities, practices, procedures, processes, practical measures and resources for implementing security policies, objectives and targets can be coordinated with existing efforts in other areas (e.g. operations, finance, occupational health and safety, environmental care).
This document provides guidelines to establish co-operative voluntary arrangements between Customs Administrations and road transport operators and/or their trade associations to enhance supply chain security and to promote trade and transport facilitation. Road transport operators, being an integrated part of the supply chain, may possibly use these guidelines in conjunction with other management systems:

- To demonstrate their commitment to security in road transport, which is an integral part of the supply chain,
- As a voluntary, internal management tool to develop, implement or improve their Security-Management System,
- To secure the application of simplified, streamlined Customs procedures.

The guidelines are intended to complement any existing national co-operative arrangements, such as those designed to address drug trafficking, illegal immigration, customs and transit fraud and extend such arrangements to include wider security aspects related to international supply chains.

---

[1] *The "High Level Guidelines for Co-operative Arrangements between WCO members and Private Industry to Increase Supply Chain Security and Facilitate the Flow of International Trade," adopted at the 3rd WCO Task Force meeting and subsequently endorsed by the WCO Council concluded, under the heading "Partnership":*

"To the extent that Customs can rely on its partners in the trade community to evaluate and address threats to their own supply chain, the risk confronting Customs is reduced. Therefore, companies that demonstrate a verifiable willingness to enhance supply chain security will benefit. Minimizing risk in this way helps Customs in performing their security functions, and in facilitating legitimate trade."

Participation in such a co-operative programme would contribute towards individual road transport operators being deemed "secure" and eligible for enhanced facilitative Customs procedures.

1.1. Principles and Objectives

Key principles for implementing these guidelines include, but are not limited to, the following:

a) Facilitation of transport and trade cannot be ignored, even when security considerations are high on the agenda. It is essential to strike a proper balance between security and the facilitation of formalities and procedures, particularly at frontiers.

b) All parties, both commercial and official, can contribute towards enhancing the security of the supply chain.

c) Security is among the highest corporate priorities for those involved in the international movement of goods.

d) Protection of legitimate trade, as well as honest traders and transport operators, should be a basic principle.

e) Communication with internal and external interested parties needs to be established, maintained and, if already in place, improved.

f) All parties in the supply chain must meet relevant legislative requirements, including those imposed by international treaties and conventions.

g) All parties should maintain the highest levels of integrity.

h) Management and employee commitment to security based on voluntary security guidelines with clear assignments of accountability and responsibility should be established when appropriate.

i) Appropriate and sufficient resources, including information supply and training should be provided to achieve the required security levels.

j) Respect of voluntary guidelines duly applied and documented should be taken into account when the liability of the transport operator is being considered.

k) Authorities should endeavour to provide adequate support (or training, advisory, audit etc.) to small and medium-sized companies (SMEs) to enable them to meet security requirements.

The objectives of these guidelines are to:

a) Promote increased co-operation between Customs Administrations and road transport operators and their trade associations.

b) Encourage the active involvement of road transport operators in enhancing cargo security in that portion of the supply chain over which they have control.

c) Encourage Customs Administrations to facilitate, to the greatest extent possible and consistent with the application of adequate controls, road transport operators' legitimate trade.

d) Minimise illegal access to, and use of, commercial trade and transport assets, systems and procedures.

e) Increase Customs' ability to detect and forestall specific attempts to commit customs offences in cargo shipments.

f) Increase Customs' ability to identify and develop substantive investigative cases involving attempts or conspiracies to commit customs offences.

g) Encourage road transport operators to allow Customs Administrations, on reasonable request, and in accordance with laws or regulations, access to commercially-held information about specific shipments, for preventive, investigative, or intelligence purposes. This access would, amongst other benefits, enable the identification of the persons directly liable for the customs offences and the taking of appropriate action against them to obtain settlement of evaded taxes and duties.

h) Assist Customs, the law enforcement community as a whole and society in general, in their efforts against these criminal elements.

1.2. Definition of Terms

Security-Management System. Set of interrelated or interacting elements to establish a security policy, objectives and measures to achieve those objectives.

Organisation. Group of people, premises and facilities with an arrangement of responsibilities, authorities and relationships.

Supplier. Organisation or person that provides a product or service, including sub-contractors.

Process. Set of interrelated or interacting activities which transform inputs into outputs.

Procedure. Specified way of carrying out an activity or a process.

Cargo Transportation Unit (CTU). Any container or closed means of conveyance intended for transport of cargo via road, rail or inland waterways, used in international traffic, of which the interior cannot be accessed other than by visibly damaging its bottom, sides, fronts, top, door or locks, or by breaking its seals.

Preventive action. Action to eliminate the cause of a potential nonconformity or other undesirable situation.

Supply chain. The entirety of processes, process steps, organisations and suppliers to get a product moved across international borders from the manufacturer to the point of delivery, as defined by the purchaser.

Premises. An area or facility under the control of the organisation that is used for the processing, storage or handling of cargo and related information.

Restricted area. An area where physical or electronic access is controlled due to the criticality or vulnerability of its contents.

Physical Security. Minimise possibility that the characteristics of cargo in a secure area are illegally changed including measures taken to guard against smuggling, sabotage, escape, attack, or other crime. This danger includes:

- Infiltration with weapons or any other dangerous substances and devices intended to harm people, property or the environment, or

- Theft of or damage to cargo.

Information Security. Minimise possibility that information in a document (paper or electronic) is accessed, distributed or changed without proper authorisation including measures taken to guard against espionage, sabotage or other crime.

Tamper. Any act, object, or practice that results in the improper alteration of information, documentation, seals, cargo or conveyances with the intent to deceive, remove or secrete.

Company Security Officer. The person designated by the organisation to be responsible for the implementation and maintenance of security measures, who liaises with the designated authorities and other parties involved on security issues.

Top management. A person or a group of persons who direct and control an organisation at the highest level.

Corrective action. Action to eliminate the cause of a detected nonconformity or other undesirable situation.

Security manual. Document specifying the security policies and procedures of an organisation.

1.3. Potential Benefits

1.3.1 Benefits for road transport operators:

a) Enhanced security of goods in the international trade and transport supply chain.

b) Participation in a co-operative programme is an indication of a “low risk” trader with a proven record of compliance with Customs legislation and regulations resulting in:

   i. Streamlined Customs procedures,

   ii. Minimum level of Customs interventions,

   iii. Reduction in delays at borders,

   iv. Optimised supply chain cost through security efficiency.

   v. More efficient international trade and transport operations.

c) Improved Customs/Business relationship.

d) Consideration in Customs enforcement proceedings.

e) Safer work environment.

1.3.2. Benefits for Customs Administrations:

a) Enhanced goods security in the international supply chain.

b) An emphasis on self-assessment and self-policing rather than Customs' verifications.

c) Improved intelligence-gathering process, risk assessment capability and better targeting of high-risk consignments.

d) Optimised use of resources.

1.4. Roles & Responsibilities

For the sake of consistency and uniformity, the following roles & responsibilities should be recognised:

1.4.1. The prime responsibility of road transport operators is the safe and secure management of goods and transport/logistic operations under their control according to existing legal rights and obligations (e.g. CMR, ADR, TIR, etc. conventions and other international rules regulating international road transport).

1.4.2. The prime responsibility of Customs Administrations is the enforcement of legislation relat ing to the cross-border movement of persons and goods.

1.4.3. Customs Administrations should strictly implement rules for admitting traders and trans port operators to certain facilitation procedures (e.g. minimum conditions and requireq ments for authorisation of transport operators to have access to customs transit systems, such as the TIR system, or to deny or withdraw such authorisation).

1.4.4. The road transport operator should not be asked to act as law enforcement entities or to contravene any applicable legislation.

1.4.5. Co-operative agreements (e.g. MOUs, agreed best practices and check lists etc.) between Customs Administrations and road transport operators and/or their trade associations should be voluntary, while not removing any existing legal obligations.

1.4.6. Customs Administrations should accept that some information in the possession of the road transport operator may be regarded as commercially confidential and require the appropriate warrant, subpoena or non-disclosure agreement. Similarly, road transport operators should treat Customs' enquiries about their personnel, facilities, means of trans- port, procedures and services as confidential. This access would, amongst other benefits, enable the identification of the person directly liable for Customs offences and the taking of appropriate action against them to obtain the settlement of evaded taxes and duties.

1.4.7. Measures employed may vary from one road transport operator/industry to another and from location to location, according to the nature and extent of the perceived threat.

1.4.8. Optimum use should be made of existing commercial systems for the provision of cargo information.

1.4.9. Customs Administrations should, to the extent possible, use the WCO Data Model for the electronic exchange of data requirements (http://www.wcoomd.org/ie/En/en.html) while accepting any other means and forms of communications from the transport company. Thus, if a road transport operator is unable to transmit data electronically, Customs Administrations should accept hardcopy documents containing the required data ele ments for a mutually agreed transitional time period, like in the framework of the TIR system.

1.4.10. The highest possible levels of moral integrity should be maintained by all personnel involved in the international supply chain.

1.4.11. Customs Administrations should use accepted risk management techniques for control and cargo security assessment purposes.

1.4.12. Customs Administrations should recognise that they have a trade facilitation role and adopt modern, simplified procedures, such as those provided for in the Revised Kyoto Convention, making these available to companies participating in co-operative pro grammes.

1.4.13. Customs Administrations should ensure that legal requirements are clear, precise and readily available and should provide a contact point for resolving queries from economic operators on the interpretation of relevant legislation.

1.4.14. Where financial guarantees are required in any Customs procedure, Customs Administrations should regard these as a positive contribution to increased security.

2. Consultation, Co-operation and Communication

2.1. Principle

Customs, other competent authorities, road transport operators and their trade associations should consult regularly on matters of mutual interest, including supply chain security and facilitation measures[2].

2.2. Objective.

To improve two-way consultation and communication between Customs, on the one hand and road transport operators and their associations, on the other, to enhance supply chain security, stimulate other potential intelligence sources, both quantitatively and qualitatively and establish procedures which contribute towards improving risk assessment.

2.3. Action Points

2.3.1. Customs Administrations should encourage regular information exchange and consultation (according to the provisions of Chapter 1 Section 1.3 and Chapter 6 section 6.8 of the Revised Kyoto Convention), at both national and local level, with all parties involved in the international supply chain to discuss matters of mutual interest including Customs regula - tions, procedures and requirements and facility and consignment security. Customs Administrations which have consultative arrangements should be prepared to co-operate with and advise other Customs Administrations on establishing similar arrangements.

2.3.2. Road transport operators and, where appropriate, their associations should provide clearly identified and readily accessible local points of contact or a corporate contact who can arrange immediate access to a local contact for all matters identified as of enforcement interest to Customs (cargo bookings, cargo tracking, employee information, etc). Equally, Customs Administrations should provide road transport operators and associations, with telephone numbers where senior Customs officials may be contacted in an emergency.

[2](Revised Kyoto Convention, Chapter 1, Standard 1.3). "The Customs shall institute and maintain formal consultative relationships with the trade to increase co-operation and facilitate participation in establishing the most effective methods of working commensurate with national provisions and international agreements."

2.3.3. Road transport operators, individually or via their association, should encourage an open and continuing exchange of information with Customs Administrations, and vice-versa.

2.3.4. Customs Administrations should establish, in consultation with road transport operators and associations, procedures to be followed in the event of queries or suspected customs offences. Persons directly liable for customs claims should be immediately identified, so that evaded taxes and duties can be collected from them. In addition, persons directly liable for customs offences should have appropriate legal action taken against them.

2.3.5. Road transport operators should notify the appropriate Customs Administration of any unusual or suspicious cargo documentation or abnormal requests for information on shipments. In this case, they should not be penalised or liable for sanctions.

2.3.6. Customs Administrations should involve road transport operators and their trade associations in developing a risk management strategy.

2.3.7. Road transport operators should provide timely notification to Customs and, where appropriate, to other official stakeholders (such as police, tax authorities, security companies or any other relevant authority/organisation), when employees discover suspect packages or unaccounted cargo. Suspected contraband packages should be secured as appropriate.

2.3.8. Customs Administrations should provide feedback on the performance of the road transport operator in addressing security issues related to the international supply chain. Specific needs of small and medium-sized companies (SMEs) should also be taken into account and addressed.

3. Education, Training and Awareness

3.1. Principle

This encompasses the education and training of personnel on security policies, encouraging alertness to any deviation from those policies and knowledge of actions to be taken in response to security lapses.

3.2. Objective

To educate and train both Customs' and road transport operator's staff, to improve their contribution to supply chain security and to raise awareness, so helping to identify suspicious circumstances.

3.3 Action Points

3.3.1. Customs Administrations should, upon request, provide information and expert advice to the security, cargo handling and documentation personnel of road transport operators, including small and medium-sized companies, to enable them to recognise and report suspicious cases (e.g. risk profile indicators such as weight discrepancies, disappearances, incongruities in payment, package construction, routing, documentation anomalies or inconsistencies).

3.3.2. Customs Administrations should offer road transport operators advice regarding the provision of appropriate assistance and educational material to individual companies to:

a) Help them assess their vulnerability to being used for criminal purposes;

b) Develop concrete plans to reduce this vulnerability; and

c) Implement these plans.

3.3.3. Road transport operators should educate their personnel, with the assistance of Customs Administrations and, where appropriate, their trade / TIR guaranteeing associations, about the dangers of becoming involved in criminal activities and customs offences. The internal sanctions applicable to employees who become involved in such offences should also refer to possible severe penalties imposed by appropriate authorities worldwide for such offences.

3.3.4. Where practicable, road transport operators should, upon request, assist Customs Administrations in gaining familiarity with relevant company internal information systems, premises and business operations.

3.3.5. Educational material and expert guidance on the identification of potentially suspect cargo should be available to security, cargo handling and supply chain personnel.

3.3.6. Personnel involved in cargo handling, cargo documentation or security should be made aware of warning signs which may indicate that other employees may be vulnerable to, or subject to, criminal coercion.

3.3.7. Customs officials should seek the advice of road transport operators and/or their trade associations regarding routine transport and consignment documentation procedures.

3.3.8. Customs and other relevant authorities are encouraged to assist the road transport industry's own initiatives, such as the development and implementation of voluntary company guidelines, best practices, training accreditation schemes and materials, to raise awareness and assist road transport operators in taking appropriate practicable and proportionate preventive measures to minimise risk or misuse of goods or vehicles for terrorist purposes.

4. Information Exchange, Access and Confidentiality

4.1 Principle

When creating or processing security documentation, both electronic and manual, ensure that information is legible and protected against the loss of data or introduction of erroneous information.

4.2. Objective

To improve access to information, ensure the timely and accurate provision of information and protect against its misuse.

4.3 Action Points

4.3.1. Each road transport operator should have a company security information document, in proportion to the scale of the associated risk, the specificity and nature of its activity and the size of the company.

4.3.2. There should be appropriate physical controls in computer areas.

4.3.3. Access to data systems should be controlled by level of job responsibility and level of information security. Employees should be trained in computer system and data security.

4.3.4 Computer systems should include processes to backup data and monitor employee use of data systems.

4.3.5 Documents should be complete, legible, accurate and submitted in a timely manner.

4.3.6 Road transport operators and Customs Administrations should maintain the confidentiality of commercial and security sensitive information, including road transport operators' security procedures.

4.3.7 Customs authorities should give priority to “single-window” or “one-stop-shop” control techniques.

4.3.8 Full and timely implementation of electronic data exchange is needed among all partners involved in Customs procedures, in particular to confirm the termination of the Customs processes, e.g. by the application of SafeTIR in the framework of the TIR system.

4.3.9 Customs Administrations should inform traders and the transport industry about trends and new patterns of fraud and criminal activities, so they make take preventive measures.

5. Consignment Security

5.1. Principle

Consignment security includes measures to prevent unauthorised access to or handling of consignments, as well as measures inhibiting illegal access to contents by, for example, the use of seals or other access monitoring measures.

5.2. Objective

To enhance the security and integrity of consignments; to enhance controls on access to the consignment at all times while it is in the road transport operator’s control; and to establish routine procedures which contribute to the security of consignments.

5.3 Action Points

5.3.1. In case of security-sensitive goods/destinations, the road transport operator should establish clear rules and instruct drivers on the most secure way of taking goods in charge, transporting and delivering them. These may include checking the integrity of loading units at interchange points, checking seals and seal numbers, checking documentation, as well as other relevant monitoring measures. In the event of a discrepancy, a record should be made of the anomaly on consignment-related documentation.

5.3.2. The road transport operator or its agent, as appropriate, should examine cargo security and control procedures to prevent access to the consignment by unauthorised persons and the incorrect manipulation or handling of shipments by authorised personnel.

5.3.3. The Customs Administration should record the seal number or other identifier of physically inspected loading units/containers on the declaration submitted to them by the cargo carrier.

5.3.4. The road transport operator should examine empty units/containers received for storage (or loading) to ensure that no modifications have been made to their structure.

5.3.5. Unless conducting a covert operation, Customs Administrations should ensure that a rep resentative of the organisation controlling the consignment is present when cargo is physically inspected or removed for inspection. However, the party with responsibility for the security of the consignment should always be notified of such an inspection as soon as possible after the event in case of subsequent liability claims.

5.3.6. When the road transport operator, for whatever reason, is not able to be present when loading or unloading, or if he is unable to check the goods loaded, this fact should be clearly mentioned in the appropriate Customs and/or transport document.

5.3.7. Upon receipt or discharge of a cargo consignment, the road transport operator or its agent should notify Customs Administrations of instances where the integrity of the consignment has visibly been breached.

5.3.8. Customs Administration should strive to address specific needs of small and medium-sized companies, by providing them with necessary advice, information, training, etc.

5.3.9. Contraband discovered by the staff of a road transport operator or its agent should be made secure with minimal handling and immediately reported according to regulations, if related to terrorism or criminal activity. (Actions and cooperation by the transport opera tor, duly applied and documented, should be regarded favourably when the transport operator's liability is being considered).

6. Security of the means of transport

6.1. Principle
Conveyance security should provide protection against the introduction of unauthorised personnel or material into the supply chain, including the areas between the links of the supply chain.

6.2. Objective
To enhance conveyance security.

6.3. Action Points
6.3.1 The road transport operator should strive to install security equipment, check it regularly and instruct drivers in its proper use.

6.3.2 Customs Authorities should pay specific consideration to security aspects when inspecting vehicles and containers for acceptance/approval for international transport operations under Customs seals.

6.3.3 The road transport operator or its agent, as applicable, should establish security and control procedures to discourage unauthorised persons from gaining access to their vehicle.

6.3.4 The road transport operator should secure internal/external compartments and panels.

6.3.5 The road transport operator should establish security and control procedures, limited to the minimum necessary for the safe and efficient working of the carrier and access to the means of transport.

6.3.6 The road transport operator should identify places where illegal or illicit goods might be concealed on board vehicles and ensure that these places are regularly inspected. Log entries should be made following such inspections indicating the areas inspected.

6.3.7 The road transport operator should have procedures for reporting on unauthorised person nel, non-manifested materials, or signs of tampering with a conveyance or vehicle.

6.3.8 Customs Administrations should strive to address specific needs of small and medium-sized companies, including providing them with necessary advice and information training related to vehicle security.

7. Security on Premises

7.1. Principle

Address security and access control issues for those premises owned, operated or controlled by the road transport operator, including security measures to ensure the security of the actual "building" and those that monitor and control the exterior and interior perimeters of the facility and access controls that prohibit unauthorised access to facilities, conveyances, loading docks, and cargo areas. If access control is not possible, increased precautions in other security aspects may be needed.

7.2. Objective

To enhance the security of premises.

7.3. Action Points:

7.3.1. The road transport operator should as far as possible:

a) Ensure that only authorised persons, vehicles and goods are permitted access to their facilities and that goods within their facilities are not tampered with.

b) Maintain appropriate peripheral and perimeter barriers.

c) Restrict access to document or cargo storage areas.

d) Develop procedures to challenge unauthorised or unidentified persons.

e) Where appropriate, maintain appropriate electronic security systems, including theft alarm systems, access control systems, closed circuit television (CCTV).

f) Clearly identify restricted areas.

g) Control and record private vehicle access to their facilities.

h) Limit the parking of vehicles (except those carrying cargo to and from facilities) to designated areas effectively segregated from active cargo handling facilities. Employee parking should be separate from visitor parking.

i) If feasible and practicable, issue a dated pass to all vehicles given one-time access to a restricted facility and limit parking to approved and controlled areas, recording license plate numbers and supply Customs with these upon request.

j) Permit only authorised personnel and vehicles displaying proper identification to be within cargo holding areas and in proximity to equipment.

k) On request, allow Customs access to security monitoring systems.

l) Subject to national legislation, provide information to Customs Administrations on request, about any sub-contractors working at their facilities, and any company supplying support services.

7.3.2. Customs Administrations should:

a) Monitor and encourage high security standards on road transport operator premises and at approved clearance points.

b) Provide advice to road transport operators on raising security standards at their facilities.

c) Arrange for reports about suspect consignments or persons to be made with minimum delay to, or interference with, the movement of legitimate trade.

d) Inform road transport operators and their associations of the latest Customs Administrations' experience and knowledge of seals and other tamper-proof devices and other security measures.

e) Address specific needs of small and medium-sized companies and provide them with the necessary advice, information training, etc.

f) Consider obtaining data on vehicles, persons etc. allowed regular access to facilities by automated means.

8. Personnel Security

8.1. Principle
Promoting the screening of employees and prospective employees, as appropriate and as provided for by national legislation.

8.2. Objective
To improve monitoring of employees and background checks on them.

8.3. Action Points:

8.3.1. The road transport operator should pay special attention when recruiting staff, including inclusion of security duties in employment contracts and job descriptions. Where national legislation permits, all reasonable precautions should be taken when recruiting new staff to check identification and references and verify they have not been previously convicted for security-related or customs offences or have a history of drug abuse, in accordance with national legislation.

8.3.2. The road transport operator should ensure that all employees receive appropriate informa tion and training on security matters.

8.3.3. Appropriate road transport operator personnel should be trained/informed to recognise warning signs that an employee may be susceptible to pressure from criminal elements and be aware of the appropriate action to be taken if such suspicions arise.

8.3.4. The road transport operator and Customs Administrations should, where appropriate, and in accordance with national legislation, conduct periodic background checks on employ ees working in security sensitive positions, noting unusual changes in an employee's apparent social and economic situation.

8.3.5. The road transport operator and Customs Administrations should ensure the moral integrity of their employees and establish a mechanism enabling the proper investigation of suspected lack of integrity.

8.3.6 The road transport operator should seek to raise awareness of security issues amongst their employees.

9. Trading Partner Security

9.1. Principle

Trading partner security extends supply chain security to the road transport operator's suppliers and customers, even though the road transport operator may not have operational control over these parties. Communication, assessment, training and continuous improvement are key components.

9.2. Objective

To strengthen security throughout the supply chain and to support current adequate supply chain security measures in place.

9.3. Action Points

9.3.1. When entering into contractual arrangements with trading partners/suppliers/contractors in an international supply chain, the road transport operator should raise its partners' aware ness of security issues and incorporate security provisions in those contracts, if the parties concerned agree.

9.3.2. Such contract provisions should encourage trading partners/suppliers/contractors to assess and enhance, if required, their supply chain security.

9.3.3 The road transport operator should avoid, as much as possible, oral or written transport contracts that foresee cash payment.

9.3.4. Customs and other authorities should provide information when requested by traders or transport operators on the reliability of their commercial partners, whenever legally possible.

9.3.5. Before entering into contractual relations, the transport operator should check the commercial details of its clients.

9.3.6. The transport operator should exercise extreme caution in case of

a) Clients offering cash incentives for the transport of goods over and above the market price;

b) Clients offering the transport of goods that have passed their "sell by date" or are past the storage date;

c) Clients offering the transport of goods with low value, making any commercial transaction uneconomic;

d) routing instructions that are illogical because they entail a detour from the direct route to the delivery point;

e) Requests for the transport of high value goods in general and, in particular, if from a company that is not normally engaged in such activities.

10. Crisis Management and Disaster Recovery

10.1. Principle

Crisis management and disaster recovery procedures include advance planning and the establishment of operation processes for extraordinary circumstances.

10.2. Objective

To minimise the impact of an incident.

10.3. Action Points

10.3.1. The road transport operator should develop and document, in conjunction with the appro priate authorities, contingency plans for emergency security situations and for disaster recovery in the event of a security incident.

10.3.2. Emergency plans should include periodic training of employees and testing of the plan.

10.3.3. Customs Authorities should strive to provide assistance to operators who are seeking to develop standard security plans and other similar security-related measures. Furthermore, application of voluntary guidelines, duly applied and documented, should be positively taken into account when the liability of the transport operator is being considered.

11. Measurement, Analyses and Improvement

11.1. Principle

An effective Security Management System should be put in place, covering security policy, security objectives, assessment of results, analysis of data, reports on security incidents, corrective and preventive actions, as well as management review. The road transport operator should establish, document and implement a Security Management System and continually monitor its adequacy in accordance with these guidelines.

11.2. Objectives

The road transport operator should plan and implement monitoring, measurement, analysis and improvement processes in order to:

11.2.1. Assess consistency with these guidelines

11.2.2. Ensure integrity and adequacy of the Security Management System, and

11.2.2. Identify areas where the effectiveness of the Security Management System could be improved.

11.3. Action Points

11.3.1. The road transport operator should make an assessment of the security risks in their operations and take appropriate measures to mitigate those risks.

11.3.2. The road transport operator should conduct regular self-assessment of its Security Management System.

11.3.3. The road transport operator should document the self-assessment procedure and the responsible parties. Where appropriate, Customs Administrations should provide self-assessment guidelines to ensure consistency.

11.3.4. The road transport operator should continuously monitor and, where applicable, measure the implementation and the effectiveness of its Security Management System. When planned results are not achieved, possible corrective action should be identified and a plan for their improvement developed for inclusion in the revised Security Management System.

11.3.5. Top management should review the Security Management System at planned intervals, to ensure its continued adequacy. Records from management reviews should be main tained and stored.

11.3.6. The management review should include assessment results, feedback from the designated parties and recommendations for possible enhancements to be incorporated in a plan for the forthcoming period to ensure continued adequacy of the Security Management System.

Working together for a better future

since 1948

International Road Transport Union, Secretariat General

3, rue de Varembé
B.P. 44
CH-1211 Geneva 20
Switzerland

Tel: +41-22-918 27 00
Fax: +41-22-918 27 41
E-mail: iru@iru.org
Web: www.iru.org

IRU Permanent Delegation to the European Union

32-34 avenue de Tervuren
Bte 37
B-1040 Brussels
Belgium

Tel: +32-2-743 25 80
Fax: +32-2-743 25 99
E-mail: brussels@iru.org
Web: www.iru.org

IRU Permanent Delegation to the Commonwealth of Independent States

Office 417, entr. 6
12, Krasnopresnenskaya nab.
Moscow 123610
Russia

Tel: +7-095-258 17 59
Fax: +7-095-258 17 60
E-mail: moscow@iru.org
Web: www.iru-cis.ru