Study on the impacts of possible European legislation to improve transport security

Final report: Impact assessment

Report for European Commission DG TREN
Report no.: 40008032-6-2 (public version)
Rev 2: final, 26 October 2005
Impact assessment

For

European Commission DG TREN
Rue de Mot 28-1/24
B-1049 Brussels

Client ref: BE1007593

Report No.: 40008032-6-1

Subject Group:

Indexing terms: Infrastructure, Risk Analysis, Supply Chain, Security, Terrorism, Transportation, Mitigation Measures

Summary:

Prepared by: Peter Mackenbach
Michiel Coolen

Verified by: Frans Houben

Approved by: Frans Houben

Date of issue: 10 October 2005

Project No: 40008032

☐ No distribution without permission from the client or responsible organisational unit (however, free distribution for internal use within DNV after 3 years)

☐ No distribution without permission from the client or responsible organisational unit

☒ Strictly confidential

☐ Unrestricted distribution
This study has been performed by:

**Det Norske Veritas**
DNV is a leading international provider of services which assist clients to manage their risks. As an independent foundation its objective is safeguarding life, property and the environment. DNV is an international organisation with a network of 300 offices spread over all the continents in 100 countries and employing 6,400 people.

And its partners:

**BMT Transport Solutions GmbH**
BMT-TS is a subsidiary of British Maritime Technology Ltd (BMT) offering strategic business advice to the transport sector and developing sustainable, efficient and effective European transport solutions.

**Port Maritime Security International**
PMSi is a subsidiary of Eurotunnel plc, providing security services for the port, maritime, rail and logistics industries.
Executive Summary

1. Identifying the problem of and need for transport security

The problem: ALL TRANSPORT IS AT RISK. While security risks relating to terrorism exist in all modes of transport and freight flows, they are not all covered by security legislation to deal with these risks. The security level of various transport modes and freight flows therefore varies significantly. Whereas maritime transport, air transport and transport of dangerous goods are covered by strict security legislation, specific land based transport modes lack any form of security legislation.

Terrorist risks are transnational in nature. Terrorism is thinking about the unthinkable.

Most Member States have not established an overall transport security policy, nor identified the most effective measures to counteract possible security risks relating to terrorism in the transport sector. The few initiatives that have been undertaken by Member States focus on physical infrastructure, while supply chain security is left virtually untouched.

Protection against terrorist risks costs money. Large sized companies have, to some extent, implemented some security measures for their own supply chain operations. However, the majority of the medium and nearly all small sized companies in the supply chains, including their employees, have neither implemented security measures nor are fully aware of terrorist risks.

EU measures can only be effective when taking account of the interdependency of:
- Various activities of companies in the market, relating to freight flows in the supply chains from manufacturer to destination.
- Policy initiatives and business capacity in relation to the possibility of law enforcement and effective execution.

The need:
The EU Council of Minister has defined a need to protect transport from security risks. Interconnectivity between the modes should be taken care of, covering the EU 25 territory and the supply chain.

In the long term a transport security dimension should cover the supply chain whereby all transport modes, freight flows and international trade are integrated under one legal framework.

While not an objective on its own, the increase of the quality of business performance due to implemented security programs can be considered a positive collateral benefit.
2. The transport security risks

Security risk is defined as the combination of:

- Vulnerability to attack, which reflects the possibility for a terrorist to attack the transport network successfully, compared to the possibility of protecting it through inherent or managed safeguards.

- Consequences of a successful attack, relating to:
  - The possible number of fatalities; and
  - The economic impact which is calculated with the following factors:
    - The reconstruction costs of the destroyed transport element
    - The disruption time of the transport flow
    - The volume of the transport flow

The systematic assessment of the transport security risks is based on the identification and assessment of a full range of foreseen possible terrorist intervention scenarios.

Based on the developed scenarios, the transport security risks can be classified into:

- **Infrastructure risks:** The terrorist has the objective to damage or destroy transport elements in order to disrupt the transport supply chain. The transport elements are in this case the terrorist’s target.

- **Supply chain risks:** The terrorist has the objective to misuse the transport supply chain as their means to create damage or fatalities. The transport elements are in this case not the target but the means. The misuse of the supply chain relate to:
  - The transport supply chain (cargo or mobile unit) is used as a means to conceal and transport various explosives, incendiary devices or nuclear devices to a location where they are unloaded or detonated;
  - The transport supply chain (cargo or mobile unit) is misused as a weapon.

3. The assets to protect with transport security?

The assets at stake are:

- **EU population.** A misuse of the supply chain could result in possible thousands of injuries and fatalities, i.e. transport reaches all 456 million inhabitants of the EU.

- **Economy - the EU industrial base.** All economic activities in the supply chain are at risk. Everyday cargo is shipped and transported to serve the needs for industry and consumers. Possible terrorist intervention can result in billions of Euros economic damage to the EU. It is estimated that the maximal cost of any terrorist attack on a European corridor cost maximal 2% of the original investment. Even so the economic damage could tally up as
high as 6.6 billion Euros for major existing transport corridors by taking out a single piece of infrastructure. However, a misuse of the transport supply chain to conceal and transport weapons of mass destruction to industrial and densely populated conglomerates can result in even higher economic damages. Nuclear detonation in a major port city could have a calculated economic damage of 200 to 500 billion euros.

Transport security can protect the assets either by reducing the consequences of a possible successful terrorist attack or by reducing the vulnerability of the transport system and supply chain to the attack.

The transportation elements, which make up the transport systems and supply chains, most vulnerable to terrorist interventions are the following:

<table>
<thead>
<tr>
<th>Transport modes</th>
<th>Rail</th>
<th>Road</th>
<th>Inland</th>
<th>Short Sea / Non-ISPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting infrastructure</td>
<td>* Tracks</td>
<td>* Highways</td>
<td>* Waterways</td>
<td>n/a = open sea. (Connecting infrastructure to the short sea port is included in other transport modes)</td>
</tr>
<tr>
<td>Nodes (transaction point)</td>
<td>* Cargo terminal</td>
<td>* Logistic terminal</td>
<td>* Inland ports/terminals</td>
<td>* Ports/Terminals</td>
</tr>
<tr>
<td>Control Systems</td>
<td>* Central Rail Traffic Management</td>
<td>* Road traffic management systems</td>
<td>* Vessel traffic management</td>
<td>* Vessel traffic management</td>
</tr>
<tr>
<td>Communication Systems</td>
<td>* Communications network / mobile network</td>
<td>* Communications network / mobile network</td>
<td>* GPS/VHF/AIS network</td>
<td>* GPS/VHF/AIS network</td>
</tr>
<tr>
<td>Power supply</td>
<td>n/a (self powered vehicles)</td>
<td>n/a (self powered vehicles)</td>
<td>n/a (self powered vehicles)</td>
<td>n/a (self powered vehicles)</td>
</tr>
<tr>
<td>Staff</td>
<td>* Driving personnel</td>
<td>* Driving personnel</td>
<td>* Driving personnel</td>
<td>* Driving personnel</td>
</tr>
<tr>
<td>Mobile units</td>
<td>* Locomotives</td>
<td>* Trucks</td>
<td>* Vessels</td>
<td>* Vessels</td>
</tr>
<tr>
<td>Cargo</td>
<td>* Non-dangerous</td>
<td>* Non-dangerous</td>
<td>* Non-dangerous</td>
<td>*Non-dangerous</td>
</tr>
<tr>
<td></td>
<td>* Explosive</td>
<td>* Explosive</td>
<td>* Explosive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Toxic</td>
<td>* Toxic</td>
<td>* Toxic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Flammable</td>
<td>* Flammable</td>
<td>* Flammable</td>
<td></td>
</tr>
</tbody>
</table>

(Consumers have been excluded from the study)

Of the above elements, cargo and mobile units are particularly vulnerable to misuse by terrorists as a weapon or transportation means for malicious cargo, because of the large number and variety of operators active in the supply chain. Approximately 4.7 million companies\(^1\) make up the supply chain.

\(^1\) Ranging from manufacturers, cargo owners, importers, forwarders, agents, transporters, loading/storage companies, maintenance companies, traffic controller, to cargo information handlers.
4. Definition of the objectives

The objective of a transport security policy is to countervail any terrorist threat.

A Community measure should consist of a framework for supply chain security. It should not limit itself to addressing specific points of the supply chain but include all these points in an appropriate way.

A Community measure should cover all cargo, thus all operators, and the infrastructure as it directly relates to the functioning of the supply chain; i.e. terminals, distribution centres, and inland ports.

Security is a state responsibility. Leaving supply chain security fully to self-regulation by industry would be irresponsible for any state, as also concluded by the Heads of State (March 25, 2004). On the other hand supply chain management is an industry’s responsibility and therefore public/private partnership is necessary.

The only way to countervail terrorism in transport security is to enhance the quality of the supply chain. It must be acknowledged that secure supply chains can never be guaranteed for 100%. However, there are many opportunities for operators in the supply chain to enhance the security of freight transport.

Any EU measure must strike a balance between highly prescriptive total security and the need to ensure a free flow of trade while allowing a gradual tightening of baseline standards.

There are many reasons militating for Community and/or common standards rules on supply chain security. Indeed there appears to be no reason why there should not be a Community framework. The market makes a strong case for a Community framework open for regular and speedy adaptation to developments.

The security performance of operators has a market value. It relates to being able to function in turbulent times, since the resilience of an organisation drastically improves its capability to recover after an incident.

5. Mitigating transport security risk

Measures have been identified which mitigate the terrorist risk relating to both the infrastructure and supply chain.

A. Securing the infrastructure

In the table below twenty mitigation measures for securing transport infrastructure are identified and sorted according to their expected cost range. For each measure the applicability / effectiveness per critical infrastructure is defined.
Mitigation Measure                  Rail & Road                   Road & Rail Bridges                      Multi Modal Terminals                        Rail Marshal ling Yards                          Rail CRT Management                                     Logistics Terminals                                   Road Terminals                                       Waterways                          Ship Locks                              Terminals - Short Sea                  Power Supply Rail Systems

M03 - Perimeter Fencing Standard       X  X  X  X  X X                  X X X X X X X
M08 - Access Control Manual           X  X  X  X X                               X X
M06 - Security Lighting               X  X  X  X X                               X X X X
M01 - CCTV Manual                     X  X  X  X X                               X X
M05 - Portal Protection Automated     X  X                                 X X
M02 - CCTV Motion Detection           X  X  X  X X                               X X
M07 - PIDS Motion Detectors           X  X  X  X X                               X X
M14 - Hazchem Management              X  X  X  X X                               X X
M17 - Security Awareness/Exercise Program X  X  X  X X X X X X X X
M20 - Computer Security Measures      X  X  X  X X                               X X
M04 - Perimeter Fencing Alarmed       X  X  X  X X                               X X
M09 - Access Control System - Automated X  X  X  X X                               X X
M10 - Traffic Inspection Manual       X  X  X  X X                               X X
M11 - Traffic Inspection - Explosive Detection X  X  X  X X                               X X
M15 - Risk Management System         X  X  X  X X X X X X X X X X X X X X
M16 - Staff Vetting & Training       X  X  X  X X X X X X X X X X X X X X
M18 - Security Guard Force            X  X  X  X X                               X X
M13 - Breakdown Recovery              X  X  X  X X                               X X
M19 - Security Dogs                   X  X  X  X X                               X X
M12 - Traffic Inspection - X-Ray Screening X  X  X  X X                               X X

Note: X = Most likely sites for deployment

Based on the applicability of the mitigation measures, cost bands have been set up on minimum / maximum basis for both simple and complex variants of the 10 most vulnerable infrastructure types (on the assumption that no security measures have been taken; where such measures have already been taken the solvent sum would be smaller).

<table>
<thead>
<tr>
<th>Mitigation Measure</th>
<th>Rail &amp; Road Tunnels</th>
<th>Road &amp; Rail Bridges</th>
<th>Multi Modal Terminals</th>
<th>Rail Marshalling Yards</th>
<th>Rail CRT Management</th>
<th>Logistics Terminals</th>
<th>Road Terminals</th>
<th>Waterways</th>
<th>Ship Locks</th>
<th>Terminals - Short Sea</th>
<th>Power Supply Rail Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>M03 - Perimeter Fencing Standard</td>
<td>X  X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M08 - Access Control Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M06 - Security Lighting</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M01 - CCTV Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M05 - Portal Protection Automated</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M02 - CCTV Motion Detection</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M07 - PIDS Motion Detectors</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M14 - Hazchem Management</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M17 - Security Awareness/Exercise Program</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M20 - Computer Security Measures</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M04 - Perimeter Fencing Alarmed</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M09 - Access Control System - Automated</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 - Traffic Inspection Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M11 - Traffic Inspection - Explosive Detection</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M15 - Risk Management System</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M16 - Staff Vetting &amp; Training</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M18 - Security Guard Force</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M13 - Breakdown Recovery</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M19 - Security Dogs</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M12 - Traffic Inspection - X-Ray Screening</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: X = Most likely sites for deployment

<table>
<thead>
<tr>
<th>Mitigation Measure</th>
<th>Rail &amp; Road Tunnels</th>
<th>Road &amp; Rail Bridges</th>
<th>Multi Modal Terminals</th>
<th>Rail Marshalling Yards</th>
<th>Rail CRT Management</th>
<th>Logistics Terminals</th>
<th>Road Terminals</th>
<th>Waterways</th>
<th>Ship Locks</th>
<th>Terminals - Short Sea</th>
<th>Power Supply Rail Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>M03 - Perimeter Fencing Standard</td>
<td>X  X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M08 - Access Control Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M06 - Security Lighting</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M01 - CCTV Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M05 - Portal Protection Automated</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M02 - CCTV Motion Detection</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M07 - PIDS Motion Detectors</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M14 - Hazchem Management</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M17 - Security Awareness/Exercise Program</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M20 - Computer Security Measures</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M04 - Perimeter Fencing Alarmed</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M09 - Access Control System - Automated</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 - Traffic Inspection Manual</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M11 - Traffic Inspection - Explosive Detection</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M15 - Risk Management System</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M16 - Staff Vetting &amp; Training</td>
<td>X  X  X  X X X</td>
<td></td>
<td></td>
<td></td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M18 - Security Guard Force</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M13 - Breakdown Recovery</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M19 - Security Dogs</td>
<td>X  X  X  X X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M12 - Traffic Inspection - X-Ray Screening</td>
<td>X  X</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The above information can be of relevance to Member States in their future decision processes and can be a basis for further work by the European Commission on identification and protec-
tion of critical transport infrastructure. The impact analysis however, will focus on improving the security of the supply chain.

B. Securing the supply chain
Based on the inventory of security risks the following feasible and effective generic mitigation measures for operators in the supply chain have been defined.

Mitigation measures to be taken by all:
1. Make an assessment of the risk that their operations are the target of terrorist interventions to determine the appropriate countermeasures, effective for the type and size of their supply chain operation.
2. Apply their mind to security.
3. Deny unauthorised access to their organisation through employee vetting.
4. Deny unauthorised access to critical working areas, e.g. maintenance areas, loading areas, storage areas, transportation areas, critical information processing areas etc.
5. Implement training and awareness programs to identify suspect behaviour.
6. Prevent use of bogus sub-contractors.

Mitigation measures to be taken where appropriate:
1. Deny unauthorised access to means of transport
2. Deny unauthorised access to cargo
3. Deny unauthorised access to confined spaces in means of transport
4. Deny unauthorised access to steering houses in means of transport
5. Deny unauthorised access to traffic control systems
6. Deny unauthorised access to information about cargo/ routes
7. Inspect confined spaces in the means of transport and cargo
8. Separate dangerous goods from other cargo
9. Reroute dangerous cargo

For each of the generic measures above, detailed functional measures, including their applicability to the different transport modes, have been defined. An overview the approximately 75 detailed measures can be found in summary appendix I.

6. The main policy options
In view of size and complexity of the markets, achieving high levels of supply chain security can only be a long-term objective, with considerable investments. Legislation, rather than non-legislative measures, is necessary to develop a common framework and establish a level playing field.

From the perspective of establishing such level playing field, an EU Regulation is recommended because of:
- Necessity to introduce common measures in all EU 25 at the same time;
- Need for mutual recognition of secure operators within the EU Member States.

In addition, most other EU security measures are also Regulations.

A two phase introduction of security in the supply chain on EU territory is proposed:
The voluntary phase, period 2006-2008.
A voluntary EC framework legislation, which encourages supply chain operators to introduce security management systems into the operations, but equally puts the industry on notice. This legislation covers the functional security requirements, as developed in this study (and as included in the ISO PAS 28000 series, see also summary appendix II). Companies can be awarded secure operator status when fulfilling these standard security requirements.

To execute this voluntary scheme three conditional instruments will be developed and implemented:
- Audit scheme (conditional)
- Enforcement scheme (conditional)
- Security Awareness programme (conditional)

In addition two of the identified requirements/measures require the development of common EU instruments because of the cross border nature of the requirements:
- Employee vetting system (supporting)
- Seal programme (supporting)

A supply chain manager approach should introduce the security management systems in the EU supply chains. One operator, generally the cargo owner responsible for the transportation of the goods, is made responsible for the supply chain, the selection of its operators and its security. In order to create a secure supply chain, this operator, known as the ‘Supply Chain Manager’ selects only certified secure supply chain partners (according to the requirements defined in this study). While each operator is responsible for implementing the security measures in their own organisations, the Supply Chain Manager will guarantee the security of the supply chain.

During the voluntary phase Member States motivate the Supply Chain Managers on setting up secure supply chains. This will lead to gradual implementation of security management in the market. Each Supply Chain Manager’s voluntary decision to implement supply chain security, makes for all participating operators the compliance to the security requirements mandatory. It will prevent massive peak implementation at the mandatory date, as seen with ISPS. A further benefit is that not just the security of individual operators can be guaranteed but also that of the whole supply falling under responsibility of one Supply Chain Manager.

To motivate ‘Supply Chain Managers’ and operators in introducing security management in their operations and supply chains, and to reward those who have done so, “green lane” programmes should be implemented by Member States. In a “green lane” programme secure op-
Secure operators will enjoy collateral business benefits. While aimed at protecting against terrorist attacks, implementation of security measures will inevitably also improve protection against theft. In addition whereas the prime objective of existing management system standards have been to improve quality and environmental performance of organisations, studies have shown that the systematic analyses of their processes and the requirements for continuous improvement have created positive side effects in business efficiencies and financial performances. For the implementation of security management systems similar effects on efficiencies can be expected.

The mandatory phase, starting in 2009.
After the voluntary roll out, the EC framework legislation will become mandatory as of 2009. This will coincide with the mandatory requirements from the revised Customs code. The mandatory EC framework will consist of similar instruments as the voluntary framework. With the exception of the “green lane” programs, which functioned as ‘carrots’ during the voluntary phase. These will be replaced by ‘sticks’ because of the obvious characteristics of a mandatory programme.

Long term perspective – after 2010:
As the supply chain is all about adding value to the manufacturing chain, thereby including customers demand within the chain, and sustainable transport the security of the consumers is a long term concern and should be taken care off. It needs further research.
7. Analysis of the impact of the policy options

Below the cost and benefit of each proposed instrument is presented. All cost figures are based on financial data as presented in chapter 6, which are derived from EUROSTAT data.

7.1: Implementing supply chain security management by industry

<table>
<thead>
<tr>
<th>Micro</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10 empl</td>
<td>&lt;50 empl</td>
<td>&lt;250 empl</td>
<td>&gt;250 empl</td>
<td>Total</td>
</tr>
<tr>
<td>4,208,300</td>
<td>424,800</td>
<td>98,000</td>
<td>19,300</td>
<td>4,750,443</td>
</tr>
</tbody>
</table>

| Share of the total freight flow* |
| 6.0% | 13.5% | 20.7% | 59.9% | 100% |

| Companies affected by legislation** |
| 4,171,245 | 391,300 | 58,906 | 4,568 | 4,626,019 |

| Share of the freight flow affected |
| 5.9% | 12.4% | 12.4% | 14.2% | 44.9% |

| Average implementation cost/company p.a. (x1000 euros) |
| 5 | 50 | 135 | 300 |

| Average maintenance cost/company p.a. (x1000 euros) |
| 3 | 39 | 131 | 304 |

| Total implementation costs (M€) |
| 19,685 | 19,657 | 7,945 | 1,371 | 48,658 |

| Total maintenance costs (M€) |
| 11,709 | 15,416 | 7,704 | 1,389 | 36,218 |

Annual costs for industry ***

| 2006 | ¼ * 48.658 = 12.165 M€ |
| 2007 | ¼ * 48.658 + ¼ * 36.218 = 21.220 M€ |
| 2008 | ¼ * 48.658 + ½ * 36.218 = 30.274 M€ |
| 2009 | ¼ * 48.658 + ¾ * 36.218 = 39.329 M€ |
| Onward | 36.218 M€ annually |

Benefits for industry

| Increased sustainability and resilience of organisations |
| Commercial advantage for service providers |
| Reduced number of cargo inspections |
| Reduction of cargo theft |
| Reduced chance on brand- and reputation damage |
| Increased efficiency and transparency |
| Common minimum security standards results in level playing field |

Benefits for the Member states

| Reduced risk of fatalities |
| Reduced risk of economic damage |
| One common approach throughout EU and across transport modes |
| Equal confidence in security of different modes and Member States. |

Possible negative security effect

| If the same security level is not achieved in the whole supply chain, then in spite of all investments, little has been achieved. Supply chain security is as strong as its weakest link. |
| Implementation of security measures creates a sense of security which may result in reduced awareness (to suspicious activities). |
| Incorrect implementation of supply chain security may create a false sense of security, Security control inspections are reduced even though the supply chain is not secure. |
| However, even correct implementation of supply chain security can create a false sense of security. 100% security cannot be achieved. |

*) Based on the relative production value of the manufacturers in each size category

**) Approximately 125,000 companies are not included in the cost assessment. They are assumed to be already participating in other EU and US customs security requirements. Through the proposed principle of mutual recognition compliance to these other security requirements also ensures compliance to the supply chain security requirements.

*** During the voluntary roll out, 2006-2009, a linear participation curve is assumed. This means each year a quarter of all companies decides to comply with the requirements. After the voluntary roll out, when the program becomes mandatory, all implementation costs will have been made and only the annual costs remain.
7.2: Audit schemes

<table>
<thead>
<tr>
<th>Share of companies affected by audit scheme*</th>
<th>Gradually growing to 4.626.019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of auditors involved</td>
<td>Growing to 7000</td>
</tr>
<tr>
<td>Cost for all Member States combined **</td>
<td>2.700 M€</td>
</tr>
<tr>
<td>Cost for per Member States (average)</td>
<td>€ 5.92 per inhabitant €2.55 per inhabitant</td>
</tr>
<tr>
<td>Cost for Industry***</td>
<td>Only when Member States decide to delegate auditing to third parties will costs have to be borne by industry. These will be of same order as for Member States (see remark below)</td>
</tr>
</tbody>
</table>

**| Annual Costs**

<table>
<thead>
<tr>
<th>Year</th>
<th>Initial</th>
<th>Annual</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>¼ * 2.700 = 675 M€</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>¼ * 2.700 + ¼ * 1.167 = 967 M€</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>¼ * 2.700 + ½ * 1.167 = 1.259 M€</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>¼ * 2.700 + ¾ * 1.167 = 1.550 M€</td>
<td></td>
</tr>
<tr>
<td>Onwards</td>
<td>1.167 M€ annually</td>
<td></td>
</tr>
</tbody>
</table>

Benefits to the Member states
- Ensuring the implementation and maintenance of the security management systems and mitigation measures.
- Creation of a secure operator label by which supply chains and operators who have successfully implemented the minimum requirements can be recognised.
- Security control measures can be focused on operators not part of secure supply chains.
- Mutual recognised security label supports a common security approach which increases predictability.
- Interconnectivity with the Known Consignor and the Authorised Economic Operator concepts in the aviation and customs sectors.

Benefits to industry
- Common EU audit scheme results in level playing field for industry.
- Common EU audit scheme allows mutual recognition and thus prevents multiple auditing.
- Secure operator label allows participating organisations to enjoy green lane treatment.
- Secure operator label allows participating organisations to positively distinguish themselves.

Possible negative security effect
- If audits are not of the same quality level throughout the EU, not only will the level playing field be disturbed, the security level also cannot be guaranteed. Creating a false sense of security.

*) Costs are calculated for when Member states decide to establish National Inspectorates. If Member States decide to delegate auditing to Recognised Security Organisations or 3rd party Certification bodies these cost will be absorbed by industry. The cost for industry will be of the same order as calculated for the Member States.

**) During the voluntary roll out, 2006-2009, a linear participation curve is assumed. This means each year a quarter of all companies decides to comply with the requirements. After the voluntary roll out, when the program becomes mandatory, all implementation costs will have been made and only the annual costs remain.
7.3: Enforcement schemes

<table>
<thead>
<tr>
<th>Coverage of EU-freight flow</th>
<th>2006-2009 (voluntary roll out phase)</th>
<th>Onward (mandatory phase)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gradually growing to spot checks on 10%</td>
<td>0-5%</td>
<td></td>
</tr>
</tbody>
</table>

| Required inspection staff | 7000 | 2000 |

| Cost for the Member States combined | 450 M€ p.a. | 50 M€ p.a. |

| Cost for the Member States (average) | € 1.00 per inhabitant p.a. | € 0.10 per inhabitant p.a. |

Benefits to the Member states
- Verify continued implementation and effectiveness of security management systems and mitigation measures.
- Resolves incorrect implementation / application of measures which may damage the effectiveness of the measures.
- Safety net under the periodic audits

Possible negative security effect
- None identified

7.4 Awareness programs

| Coverage of EU-freight flow | Through trade associations, industrial leaders and national governments 100% of companies are to be involved in awareness programs |

| Cost for the Member States | None |
| Costs for industry | Operational costs for running awareness programs included in costs for implementing security management |
| Cost for the EC | 2 M€ in 3 years |

Benefits to the Member states
- Continued awareness about the risk incurred by the supply chain and the need for compliance to security regulations and systems.

Benefits to industry
- Awareness among employees supports positive implementation of security management
- Employee awareness supports employee participation in identifying suspicious behaviour

Possible negative security effect
- If the programmes are not continuously repeated in an effective manner the awareness level will reduce

7.5 Employee vetting system

| Coverage of EU-freight flow | Estimated 10% |

| Cost for the Member States | None |
| Cost for industry | The employee vetting system supports the drafted security measure “employee vetting”. Costs for the system are carried by the vetting organisations which collect vetting fees from the operators. The alternative is for the operators to perform the vetting themselves, which result in higher costs because of multiple vetting. |

Benefits to Industry
- Mutual recognition secure employees.
- Prevention of multiple vetting of employees.
- Reduction of cost for vetting of staff members with high mobility, in the order of 800 million euros. Employees only need to be vetted annually instead of an estimated 4 times per year with each job change.

Possible negative security effect
- If the vetting system is not properly secured, the data may be abused by third parties.
7.6 European seal programme

<table>
<thead>
<tr>
<th>From 2006 onwards</th>
<th>Growing to 100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of EU-freight flow</td>
<td>None</td>
</tr>
<tr>
<td>Cost for the Member States</td>
<td>None</td>
</tr>
<tr>
<td>Cost for the EU</td>
<td>Minor costs are necessary to translate the standard to legislation</td>
</tr>
<tr>
<td>Cost for industry</td>
<td>Application of seals are part of the drafted security requirements for which the costs have been calculated in 7.1. There are no financial implications caused by the seal standardisation programme. Its only intention is to allow better compatibility.</td>
</tr>
<tr>
<td>Benefits to Member States</td>
<td>• Is conditional for verification if security has been violated en route</td>
</tr>
<tr>
<td>Possible negative security effect</td>
<td>• If the applied seals are not of the right quality and do not meet the technical specifications, there will be a possibility of fraud. The cargo may look secure but is all but secure and thus creates a false sense of security.</td>
</tr>
</tbody>
</table>

8. Final conclusions

The recommended measures cost money and bring rewards. Measures for transport security help to make Europe more secure. They also aim at bringing the various security levels between the different transport modes and freight flows more in coherence with each other. For industry, transport security measures are not only investments in security but also in the quality of their operations. They improve sustainability and resilience of organisations and enhance their business performance; through improved commercial positioning and business efficiency.

Investments for EU Member States

Member States must make decisions whether they wish to perform auditing themselves or whether they want to delegate the auditing function to Recognised Security Organisations or to Independent 3rd party certification bodies.

When Member States decide to perform the audits themselves it is estimated that they will spend approximately 6,00 Euro per inhabitant for the initial audit of all operators, to the total cost of 2.7 Billion Euros for the whole EU. These costs are spread over the voluntary roll out phase. Once the supply chain security requirements become mandatory all operators should be compliant and all initial audits should have been completed. Subsequently the Member States will spend 2,50 Euro per inhabitant annually, tot the total of 1,17 Billion Euros annually, for the years thereafter to periodically re-audit the operators. The costs for re-audit will gradually build up during the voluntary roll out phase, as more operators become compliant secure operators, to the eventual level of 2.50 Euro per inhabitant.

To verify initial implementation and to ensure that security management is upheld around 6.000 to 7.000 auditors are needed. Considering the capacity constraints this may create for most Member States the use of external auditing organisations which possess in-house expertise on transport security should be considered. Delegation of the audits will be cost neutral to Member States since the cost will be absorbed by industry. Costs to Member States would be limited to supervising and managing the auditing programme. The cost for industry would be approxi-
mately 2,7 billion Euros for the initial audits and 1.2 billion Euros annually for the periodic audits.\(^2\)

Enforcement, which acts as a safety net under the periodic audits, costs the Member States during the voluntary roll out phase an estimated 450 Million Euros annually, or approximately 1.00 Euro per inhabitant annually. During this phase the enforcement program has both the function to ensure continuous compliance, through spot checks, as well as create sufficient level of scrutiny for the non participating operators to make the ‘green lanes’ and thus participation attractive. During the mandatory phase, ‘green lanes’ become obsolete, therefore the only function remaining are the spot check inspections as safety net for the periodic audits. Because high level of confidence in the audits is assumed through governmental auditors or recognised third parties, the inspections can be reduced to an estimated cost of 50 Million Euros per annum for the total EU.

The number of inspectors to enforce implementation in the voluntary roll out phase is around 7,000, which is reduced to some 2,000 during the mandatory phase. Inspections need to be performed by traffic police, transport and labour inspectorates so that these normally can not be delegated.

Investments for EU industry (to introduce security management)

In the table below the per company investment and annual costs for implementing security management are expressed in \(\text{k€}\).

**Cost per company in 1000 €**

<table>
<thead>
<tr>
<th></th>
<th>Investment</th>
<th>Annual cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro</td>
<td>Small</td>
</tr>
<tr>
<td>Rail repair/maintenance shops</td>
<td>&lt;10 empl.</td>
<td>&lt;50 empl.</td>
</tr>
<tr>
<td>Rail transport</td>
<td>63</td>
<td>139</td>
</tr>
<tr>
<td>Road transport</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Rail transport</td>
<td>67</td>
<td>194</td>
</tr>
<tr>
<td>Inland shipping</td>
<td>8</td>
<td>47</td>
</tr>
<tr>
<td>Warehousing</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Other logistic support</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Manufacturers NACE Gr D</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Construction NACE Gr E</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Average</td>
<td>5</td>
<td>50</td>
</tr>
</tbody>
</table>

The drafted security measures are a combination of hardware, system and organisational measures. The hardware measures tend to have high investment cost compared to their annual cost, the costs for system measures are roughly equal while the organisational measures tend have high annual cost compared to their investment cost.

---

\(^2\) TAPA, CTPAT and STAIRSEC are all programs based on periodic auditing to ensure a continual compliance and maintenance of the security systems. Auditing can be considered a form of formal and structured enforcement. Where enforcement, as defined in this study is generally based on periodic spot checks to verify compliance to the requirements, auditing verifies the maintenance and continual effectiveness of the security system. Auditing and re-auditing is also widely used for the implementation of other management systems such as quality, safety and environment.
Through the mix of security measures, the investment costs required for implementing security management tally up to be approximately equal to the annual cost, as can be seen in the table above. As a result there is no investment peak which needs to be recuperated over subsequent years. The investment in the first year is as large as the annual costs in subsequent years.

In their very nature, security investments are first and foremost cost elements and do not directly increase revenue. However, this simple short term approach disregards the considerable risks run by operators if and when security incidents happen:
- disruptions to commercial activities;
- product adulteration;
- brand destruction are well within the realm of imagination.

Besides the implementation of the security measures will contribute to reduced theft, efficiency improvements and market benefits.

It is, of course, correct to point out that benefits are difficult to measure where no incidents occur. Operators can make these investments when they know in advance whether their investments are warranted and that requirements in the various Member States are as uniform and predictable as possible.
## Table of Contents

1.0 **INTRODUCTION AND BACKGROUND** .................................................................3

1.1 **INTRODUCTION** .................................................................................................3

1.2 **DEVELOPMENTS** ................................................................................................4

1.2.1 International initiatives .........................................................................................4

1.2.2 US initiatives .........................................................................................................4

1.2.3 EU initiatives .........................................................................................................5

1.2.4 Policy initiative versus legislation .........................................................................5

1.3 **WHAT ARE THE ISSUES?** ...................................................................................6

1.4 **WHAT IS THE GOAL?** ........................................................................................6

1.5 **PRESENT STATUS IN THE MEMBER STATES** ..................................................9

2.0 **ASSESSMENT OF THE TRANSPORT SECURITY RISKS** ...................................11

2.1 **INTRODUCTION** .................................................................................................11

2.1.1 Approach to security risk management .................................................................11

2.1.2 Assets at stake .......................................................................................................11

2.1.3 Security risk matrix .............................................................................................12

2.2 **TERRORIST INTERVENTION SCENARIOS** .......................................................12

2.2.1 Transport elements at risk ....................................................................................12

2.2.2 Terrorist intervention methods .............................................................................13

2.2.3 Terrorist Intervention Database ............................................................................14

2.3 **TRANSPORT SECURITY RISKS** .......................................................................14

2.3.1 Infrastructure risks .............................................................................................15

2.3.2 Supply chain risks ..............................................................................................16

2.4 **RISK TO EUROPE** ............................................................................................18

3.0 **MITIGATING THE RISK TO INFRASTRUCTURE** ...............................................19

3.1 **VULNERABILITY OF AND MITIGATION MEASURES FOR THE INFRASTRUCTURE** 19

3.2 **INVESTMENTS NEEDED TO SECURE THE INFRASTRUCTURE** ......................20

3.3 **THE VULNERABILITY ASSESSMENT TOOL** ....................................................20

3.4 **A SAMPLE SECURITY PLAN TO PROTECT INFRASTRUCTURE** ....................20

4.0 **MITIGATING THE RISK TO THE SUPPLY CHAIN** ..........................................21

4.1 **APPROACH** .......................................................................................................21

4.1.1 Event trees .........................................................................................................21

4.1.2 Root causes .........................................................................................................21

4.1.3 Defining mitigation measures ..............................................................................22

4.2 **GENERIC OVERVIEW OF MITIGATION MEASURES** ....................................23

4.2.1 Minimum mitigation measures ...........................................................................24

4.2.2 Possible measures in case of imminent threats ....................................................31

4.2.3 Contingency measures .......................................................................................33

4.3 **CURRENT INITIATIVES** .....................................................................................35

4.4 **DETAILED SUPPLY CHAIN SECURITY MANAGEMENT REQUIREMENTS** ........35

4.5 **ACCOMPANYING INSTRUMENTS** ...................................................................41

5.0 **REQUIRED FRAMEWORKS** ..............................................................................43

5.1 **DEVELOPING SECURITY MANAGEMENT WITHIN EU SUPPLY CHAINS** ........43

5.1.1 Applicability of the supply chain security requirements ......................................43

5.1.2 Security responsibilities: public/private partnership ..........................................43

5.1.3 Implementation approach of security in the supply chain ....................................44

5.1.4 Relation to existing security schemes ....................................................................49

5.2 **ENSURE SUCCESSFUL IMPLEMENTATION** ..................................................49

5.2.1 Implementation through audit .............................................................................50
6.0 COST AND BENEFITS OF PROTECTING THE SUPPLY CHAIN.................................................................63

6.1 COST TO INDUSTRY FOR IMPLEMENTING SECURITY MANAGEMENT..............................................63
6.1.1 Number of enterprises involved .................................................................................................63
6.1.2 Cost per company .......................................................................................................................65
6.1.3 Total cost for industry in mandatory scheme .............................................................................67
6.1.4 Total cost for industry if requirements remain voluntary .........................................................68

6.2 THE COST TO MEMBER STATES FOR IMPLEMENTING LEGISLATION.............................................70
6.2.1 Implementation of security management throughout the supply chain .....................................70
6.2.2 Enforcement ..............................................................................................................................73

6.3 OTHER COSTS.....................................................................................................................................74
6.3.1 Awareness campaigns ................................................................................................................74
6.3.2 The employee vetting system ......................................................................................................75
6.3.3 EU Seal programme ....................................................................................................................75

6.4 BENEFITS TO INDUSTRY .................................................................................................................76
6.4.1 Implementing security management ............................................................................................76
6.4.2 Audit: verification of implementation .........................................................................................80
6.4.3 Awareness programs ..................................................................................................................80
6.4.4 Employee vetting system ...........................................................................................................80
6.4.5 European seal programme .........................................................................................................81

6.5 THE BENEFITS FOR MEMBER STATES ............................................................................................81
6.5.1 Implementation of supply chain security management ..............................................................81
6.5.2 Audit: verification of implementation .........................................................................................82
6.5.3 Enforcement ...............................................................................................................................82
6.5.4 Awareness programs ..................................................................................................................82
6.5.5 European seal programme .........................................................................................................82

7.0 CONCLUSIONS & RECOMMENDATIONS..........................................................................................83

7.1 CONCLUSIONS..................................................................................................................................83
7.2 RECOMMENDATIONS .......................................................................................................................85
7.2.1 Supply Chain security management .........................................................................................85
7.2.2 Audit scheme ..............................................................................................................................86
7.2.3 Enforcement scheme ..................................................................................................................87
7.2.4 Awareness programs ..................................................................................................................88
7.2.5 Employee vetting system ...........................................................................................................89
7.2.6 Seal programme ..........................................................................................................................90

REFERENCE MATERIALS

SUMMARY APPENDIX I: DETAILED SUPPLY CHAIN REQUIREMENTS ......................................................93

SUMMARY APPENDIX II: ISO PAS 28000 SERIES ..................................................................................101

REPORT APPENDIX A: INFRASTRUCTURE SECURITY ASSESSMENT REPORT TEMPLATE ..........129

REPORT APPENDIX B: GENERIC INFRASTRUCTURE SECURITY PLAN TEMPLATE ..........................137

REPORT APPENDIX C: CURRENT INITIATIVES .....................................................................................165

REPORT APPENDIX D: COST OF SECURITY MEASURES ..................................................................181

REPORT APPENDIX E: TAPA REQUIREMENTS ....................................................................................219

Reference to part of this report which may lead to misinterpretation is not permissible

MANAGING RISK
1.0 Introduction and background

1.1 Introduction

Following the terrorist attacks on the World Trade Centre and Pentagon on September 11th 2001 and the Madrid commuter trains on March 11th 2004, a broad range of security measures has been launched. World wide it is recognised that the transportation system, which is a life line to the world economy, is extremely vulnerable to terrorist interventions which may cause massive numbers of casualties or horrendous economic damage.

Security in maritime and air transportation, including that of (air)ports has been tightened and the role of customs is rapidly expanding from that of collector of import duties to that of security inspectorate of import and export cargo.

Protection against terrorism is a priority for the European Union (EU), and one of the measures being considered is to develop new EU legislation to improve the security of surface transport, in particular the transportation supply chains which do not cross the outside borders of Europe. The objective of this new legislation is to ensure a common security approach by all Member States based on reciprocity, resulting in equal treatment by enterprises throughout Europe and avoiding the introduction of new trade barriers within the EU because of unilateral measures taken by single states.

In order to support the development and implementation of such legislation and ensure cooperation by the stakeholders, the European Commission by means of the DG Energy and Transport (DG TREN) commissioned in 2004 a study on the foreseen impacts of possible transport security legislation.

For this impact study DG TREN requested detailed, concrete and practical input to the development of EU surface transport security legislation, based on a systematic risk assessment which will form the basis for cost benefit analysis of possible security measures for the whole EU.

The study has been performed by a consortium headed by Det Norske Veritas BV, including DNV Consulting, BMT Transport Solutions GmbH, and Port Maritime Security International Ltd. Unless otherwise attributed, conclusions and judgements in this report are the views of the project team i.e. from DNV and its partners.

The study methodology applied by DNV and its partners is summarised in five steps:
1.2 Developments

The September 11th 2001 terrorist attacks in the US on the World Trade Centre and Pentagon drastically changed the view on how vulnerable the industrialised world can be for atrocities, performed by people who want to achieve their political or religious objectives or live their frustrations through performing terrorist acts.

This vulnerability to terrorist interventions was reaffirmed on March 11th 2004 when terrorist detonated nearly simultaneously 10 bombs in four commuter trains in Madrid. In particular the vulnerability of Europe’s (land based) transport systems became apparent in the attack

The maritime sector was, since terrorists attacked the American destroyer USS Cole on October 12th 2000 and the oil tanker MV Limburg on October 11th 2002, already well aware of the vulnerability of sea transport.

1.2.1 International initiatives

Following 9/11, the airline industry, which already had a long history of terrorist interventions, even further tightened up its existing security legislations. In addition slowly progressing initiatives within IMO (the International Maritime Organisation) were accelerated resulting in the adoption of a new chapter 9 in the SOLAS convention (the UN convention on Security of Life at Sea) making security provisions, as formulated in the International Ship and Port Security code, on board vessels and in sea ports compulsory as from the 1st of July 2004. The EU has, accordingly, imbedded the ISPS security provisions in its own maritime and port security regulations.

Realising that securing maritime transport requires evidence that cargo does not contain terrorist implanted goods, and that thorough cargo inspections at the entrance of sea ports would obstruct international trade, IMO requested the World Customs Organisation (WCO) to develop measures which should enhance the security of the international supply chain. A similar request was addressed to the WCO by the leaders of the G8 countries.

In response to these requests the WCO in June 2002 installed its Security Task Force. Based on the work of this task force a framework of standards to enhance supply chain security has been developed, ready for implementation by the international custom community.

1.2.2 US initiatives

In the meantime the US unilaterally has taken a number of initiatives to reduce the possibility that cargo, imported into the United States by air, sea or road contains illegitimate goods which can be instrumental for terrorist interventions. The most relevant are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against terrorism (C-TPAT) programme.

The CSI programme aims at pushing America’s borders away from the US. In the main container ports around the world US custom officials are located which, in cooperation with the local customs perform risk assessments and decide which US bound containers will be inspected.
C-TPAT is a voluntary programme that has formulated security requirements which importers into the US have to imply on themselves and their partners in the supply chains. Parties which can demonstrate that they operate secure supply chains into the US are rewarded by a Green Lane through customs, i.e. they are subjected to less customs inspections when their goods arrive in the US. Larger European exporters are seeking compliance with the C-TPAT programme, but US customs are criticised by the US Government Accountability Office that the system is not offering value for money because of lack of verification whether applicants, who have been honoured with Green Lane treatment, really comply.

1.2.3 EU initiatives

Within the EU the Revised Customs Code has been developed, in line with the C-TPAT programme and the Framework for Standards of the WCO. The Revised Customs Code (EC No. 648/2005) is expected to be fully in force in 2009. Within this code the principle of Authorised Economic Operator (AEO) is introduced. An AEO will be subject to reduced customs inspections when he complies with the administrative rules and the supply chain security requirements as defined by the code. The EC aims to promote the AEO concept internationally, thus resulting in international agreements between the EU and various countries. The process to arrive at reciprocity between the US and EU customs to accept each others authorisations in due course has already started.

The AEO concept means that cargo passing through airports, sea ports or otherwise crossing the outside borders of the EU will be subject to inspections for illegal (terrorist) goods and that operators which are going to comply with the revised EU customs and got awarded AEO status will get a “Green Lane” through customs, implying reduced inspections and delays.

Other EU initiatives include:

- EU Regulation on aviation security (EC No. 2320/2002 of 16 December 2002). Further tightening of the European aviation security legislation as a result of the 9/11 attack in the United States
- EU Communication on critical infrastructure (COM (2004) 702 final of 20 October 2004). This Communication announces that a European programme for the protection of the critical infrastructures (programme “EPCIP”) will be proposed in 2005.

1.2.4 Policy initiative versus legislation

While a majority of the US initiatives can be labelled as policy initiatives without legal status (Only the 24 hour rule in the US has a legal base), most of the EU initiatives relate to legislation. Policy initiatives are generally voluntary programs which have no legal basis and are non binding. They contain recommended measures which industry are free to implement. Often implementation is rewarded in some way to stimulate participation. Legislations on the other hand have a legal basis and are binding to all participants as defined in the legislation.

The US initiatives, implemented under the Department of Homeland Security, are however often criticised for their limited effectiveness because of their non binding status. It is believed
that only through stringent binding policies effective implementation of measures can be assured.

1.3 What are the issues

None of the initiatives as mentioned above address the security of supply chains within custom borders, e.g. within the European Unions geographical area.

Considering that for all of the renowned terrorist attacks against the industrialised world (Madrid bombing in 2004, Bali bombing in 2002, Oklahoma bombing in 1995, the World Trade Centre bombings 1993 and 2001) materials were used for which terrorists had not needed to cross borders. This implies that together with a host of other measures, ensuring that the national supply chains are not used to transport terrorist goods or to perform terrorist acts is essential.

Based on the priority which the EU gives to combating terrorism the development of an EU Legislation on Supply Chain Security therefore is an essential step.

What needs to be considered when developing such legislation is:

- The legislation should be implemented similarly and simultaneously by all Member States, to ensure that no single county sustains commercial advantages or disadvantages compared to other Member States.
- The legislation should define the right balance between security and the economic consequences it creates.
- The legislation should formulate effective and realistic requirements to trade and industry as well as to the Member States and be based on cost-benefit analyses to ensure that the most cost effective solution has been chosen.
- The legislation should be based on a thorough risk analysis of the potential hazards in the intra EU supply chain to avoid as much as possible knee-jerk reactions of the individual Member States.
- The legislation should ensure that supply chain security management throughout the EU is harmonised to an extent that recognition of companies as being secure operators should be acknowledged and accepted by the other Member States.
- The legislation should formulate requirements which ensure that supply chains within the EU are having the same level of security as cargo traffic by road, rail, air and sea, crossing the outside borders of Europe.
- The legislations should be adopted by trade and industry as a meaningful contribution to their operation and allow them sufficient time to implement it in responsible manner.
- The legislation should avoid as much red tape as possible.
- The legislation can take the form of a regulation or a directive.

1.4 What is the goal

The goal of this study is to make analyses and provide recommendations to the European Commission which allows them to draft legislation with to the maximum takes account of the issues mentioned above.

Therefore the study has taken the following approach:

1. Make an extensive assessment of the risks of terrorist interventions in European inter-modal transport and the infrastructure it uses.
26 October 2005  
Impact assessment (final)  
European Commission DG TREN

- PUBLIC VERSION -  
Reference to part of this report which may lead to misinterpretation is not permissible

a. Through a systematic risk inventory.  
b. By defining worst case scenarios.

2. Make an identification of existing measures to enhance supply chain security and the state of the art in securing the infrastructure within the EU-25 countries.

3. Define which organisational and physical measures that contribute to improved security of the supply chain through:  
a. Identification of common threats.  
b. Development of measures and instruments to prevent or mitigate these threats  
c. Cost-benefit analysis.

4. Identify which organisational and physical measures enhance the security of infrastructure through:  
a. Definition of economic critical corridors.  
b. Definition of vulnerabilities of critical infrastructure elements.  
c. Identification of mitigation measures.  
d. Investment analysis.

5. Propose which coordination or control should be organised at a European level and which legal or other frameworks can implement security measures within the Member States of the EU.

- The scope for the study can be defined as follows: The study covers “surface” transport modes, i.e.  
  - Rail.  
  - Road.  
  - Inland waterways and  
  - Short-sea shipping.  

Air and maritime transport, as well as transport flows passing the outside borders of the union have not been included in this study since they are covered by existing or developing security regimes. Also transportation by pipeline is not covered by this study.

- The study only addresses freight transport. Passenger transports are only considered where it may be affected by security incidents initiated by the freight transport. Furthermore, the study does not address energy distribution or data communications.

- The study focuses in particular on the transportation supply chain, i.e. cargo travelling on one or more modes of transport. Cargo may be itemised in which case it will primarily travel in ISO containers or in swap bodies and trailers. Bulk cargo is also covered – with a particular focus on hazardous substances.

Figure 1.3: Sample supply chain
The study covers the whole supply chain between production and final destination before being delivered to the consumer.

- The start of the supply chain for this study is defined by the moment from which it is possible for the terrorist to realise an intervention which can have an impact on the supply chain. This is determined by the moment at which it is possible for the terrorist to conceal explosives or devices in the supply chain (either at point of loading or production, depending on the product).

- The end of the supply chain is defined as the last distribution centre before the cargo is transported to local retail outlets or the customer. The distribution network from the final distribution centre to the retailer or consumer is so fine meshed that the implementation of adequate measures is to be considered unrealistic.

For the purpose of the study, “transport security” is defined as the total of preventive measures (including human and material resources) intended to protect transport infrastructure, vehicles, systems, passengers, cargo and workers against unlawful acts. This study addresses security against terrorism.
1.5 Present status in the Member States

An inventory has been made of the status of development regarding securing the supply chain and securing the infrastructure within the Traffic Departments of the different Member States. A summary of the results of this inventory is given in figure 1.4 below.

<table>
<thead>
<tr>
<th>Infrastructure-Orgaisation</th>
<th>Austria</th>
<th>Belgium</th>
<th>Czech Republic</th>
<th>Denmark</th>
<th>Estonia</th>
<th>Finland</th>
<th>France</th>
<th>Germany</th>
<th>Ireland</th>
<th>Italy</th>
<th>Latvia</th>
<th>Lithuania</th>
<th>Luxembourg</th>
<th>Malta</th>
<th>Netherlands</th>
<th>Poland</th>
<th>Portugal</th>
<th>Slovak Republic</th>
<th>Slovenia</th>
<th>Spain</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have authorities been assigned who shall protect the countries infrastructure?</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Is cross departmental coordination in place to coordinate security initiatives?</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>P</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Are changes in the present security regime planned?</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infrastructure-Protection</th>
<th>Austria</th>
<th>Belgium</th>
<th>Czech Republic</th>
<th>Denmark</th>
<th>Estonia</th>
<th>Finland</th>
<th>France</th>
<th>Germany</th>
<th>Ireland</th>
<th>Italy</th>
<th>Latvia</th>
<th>Lithuania</th>
<th>Luxembourg</th>
<th>Malta</th>
<th>Netherlands</th>
<th>Poland</th>
<th>Portugal</th>
<th>Slovak Republic</th>
<th>Slovenia</th>
<th>Spain</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have infrastructural elements been defined which are prone to terrorist interventions?</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Are consequences of terrorist attacks on infrastructure been based on a systematic risk assessment?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Have critical infrastructural elements been defined?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Have mitigation measures been defined for critical infrastructure?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Has a list been made summarising all bridges and tunnels?</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Does staff operating critical infrastructure need to be screened?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Have different threat levels been defined?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supply Chain-Orgaisation</th>
<th>Austria</th>
<th>Belgium</th>
<th>Czech Republic</th>
<th>Denmark</th>
<th>Estonia</th>
<th>Finland</th>
<th>France</th>
<th>Germany</th>
<th>Ireland</th>
<th>Italy</th>
<th>Latvia</th>
<th>Lithuania</th>
<th>Luxembourg</th>
<th>Malta</th>
<th>Netherlands</th>
<th>Poland</th>
<th>Portugal</th>
<th>Slovak Republic</th>
<th>Slovenia</th>
<th>Spain</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have requirements been formulated regarding security management systems?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Have requirements been formulated regarding the security of mobile units?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Have requirements been formulated regarding screening of security sensitive staff?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Are there other organisations than customs that perform security inspections on cargo?</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Have different threat levels been defined?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Are changes in threat level communicated to the logistic industry?</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contingency plans</th>
<th>Austria</th>
<th>Belgium</th>
<th>Czech Republic</th>
<th>Denmark</th>
<th>Estonia</th>
<th>Finland</th>
<th>France</th>
<th>Germany</th>
<th>Ireland</th>
<th>Italy</th>
<th>Latvia</th>
<th>Lithuania</th>
<th>Luxembourg</th>
<th>Malta</th>
<th>Netherlands</th>
<th>Poland</th>
<th>Portugal</th>
<th>Slovak Republic</th>
<th>Slovenia</th>
<th>Spain</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have contingency plans for supply chain incidents been defined?</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Have risk assessments been used to develop contingency plans?</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Figure 1.4: position of Member States re transport security

\[1\] In spite of intensive efforts it proved to be impossible to obtain relevant information from the Traffic Department of four Member States (Greece, Hungary, Malta and Cyprus), however the results from the interviews with the remaining countries provided sufficient information to get a general picture of the maturity of the response to terrorist threats within the EU25.
In general it can be concluded that the awareness about the need for a better response to security threats is increasing.\(^4\)

Whereas only 2/3 of the Member States indicated that there is a centralised function in place to coordinate the security initiatives, as spread over the different departments, the dispersion of responsibilities was stated by almost all countries to be a stumbling block to effective and efficient implementation of planned measures. Only in countries where this coordination was supported by a specialised organisation, like in the UK and Germany, implementation was stated to be running reasonably smoothly.

Whereas all countries have developed contingency plans to respond to major incidents that may occur with their bridges or tunnels only 14 Member States stated to have given thought to terrorist actions against their infrastructure. Of these countries 11 have mentioned that they have defined which infrastructural elements are critical and that mitigation measures have been defined. Only 9 countries stated that this definition was based on a systematic risk assessment.

Noteworthy is that, apart from Germany, none of the countries required that the operators of infrastructural elements like bridges, locks etc. were subjected to background checks.

Important is the conclusion that none of the Member States has defined any requirements towards the security of the supply chain itself. Some countries indicated that they have been starting to think about this but that they are waiting for the outcome of this study and the legislation which the EC is going to draft.

\(^4\) The interviews were conducted in the spring of 2005, well ahead of the bomb attacks on London’s public transport system in July 2005.
2.0 Assessment of the transport security risks

The assessment of transport security risks forms the basis of the impact study. Through a systematic risk analysis possible terrorist intervention scenarios are identified to determine the security risk to the European transport system. Based on these scenarios appropriate mitigation measures will be developed.

2.1 Introduction

2.1.1 Approach to security risk management
The presumed aim behind terrorist actions is to achieve political, religious or ideological goals through exercising political pressure on governments. This political pressure is energised by:

- Creating fear and/or influencing public opinion through the mass media by causing large numbers of injuries or fatalities or spectacular damage to the transportation infrastructure.
- Causing substantial economic damage by destruction and/or putting out of use for a considerable period of time vital parts of the transportation supply chain.

In general, risk is defined as the combination of the likelihood and consequence of an unwanted event. The likelihood of a terrorist attack is, however, difficult to evaluate since for security assessments little casuistic information is available. Terrorist acts follow their own, often unpredictable rationale and not historical statistics. Also the objective of this study is not to assess in a quantitative way the risk posed by terrorist attack. Please also note that the likelihood of a terrorist attack is very sensitive to the local and global political situation, which is outside the scope of this study. This report therefore assumes that terrorist attacks can occur anywhere in the EU and that the likelihood – here called possibility – is influenced by the vulnerability of location. So the present study addresses only the probability of such an attack being successful, which reflects the lack of protection or vulnerability of the transport network at the chosen point.

When assessing the risks of accidents, the most severe events usually have the lowest probability of occurrence. However, from the terrorist’s point of view, the most severe events are the most effective at achieving their aims, and hence may be the most likely points of attack. Nevertheless, the probability of a successful attack is still related to the vulnerability of the transport network at that point.

2.1.2 Assets at stake
The assets at stake are:
- **EU population.** A misuse of the supply chain could result in possible thousands of injuries and fatalities, i.e. transport reaches all 456 million inhabitants of the EU.
- **Economy** - the EU industrial base. All economic activities in the supply chain are at risk. Everyday cargo is shipped and transported to serve the needs for industry and consumers. Possible terrorist intervention can result in billions of Euros economic damage to the EU.
2.1.3 Security risk matrix

Therefore, in the present study, security risk is defined as the combination of:

- Vulnerability to attack, which reflects the possibility for a terrorist to attack the transport network successfully, compared to the possibility of protecting it through inherent or managed safeguards.

- Consequences of a successful attack, which is defined as:
  - The possible number of fatalities; and
  - The economic impact, which is calculated with the following factors:
    - The reconstruction costs of the destroyed transport element
    - The disruption time of the transport flow
    - The volume of the transport flow

Both factors combine to form the security risk matrix as applied in this study to assess the identified terrorist intervention scenarios (figure 2.1). In the matrix the economic impact is expressed only in terms of the disruption time.

![Security risk matrix](image)

The consequences focus on fatalities and down time from a generic point of view and do not take location specific situations into account.

2.2 Terrorist intervention scenarios

2.2.1 Transport elements at risk

The transport elements, which make up the transport systems and supply chains, most vulnerable to terrorist interventions are categorised in three groups:

- **Infrastructure**: All fixed infrastructure used for transporting the cargo.
- **Operational elements**: All elements which facilitate the transportation of cargo over the infrastructure.
- **Cargo**: The actual objects to be transported which includes different types of cargo which can be manipulated in different ways to serve terrorist interventions.
### Transport modes

<table>
<thead>
<tr>
<th>Connecting infrastructure</th>
<th>Rail</th>
<th>Road</th>
<th>Shipping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnels</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridges/viaducts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switches/Rail junctions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highways</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnels</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridges/viaducts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Junctions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Waterways</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ship locks / lifts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aqua ducts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* n/a = open sea. (Connecting infrastructure to the short sea port is included in other transport modes)

<table>
<thead>
<tr>
<th>Nodes (transaction point)</th>
<th>Rail marshalling yards</th>
<th>* Logistic terminal</th>
<th>* Inland ports/terminals</th>
<th>* Ports/Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cargo terminal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rail marshalling yards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Infrastructure

- Tracks
- Tunnels
- Bridges/viaducts
- Switches/Rail junctions
- Highways
- Tunnels
- Bridges/viaducts
- Junctions
- Waterways
- Ship locks / lifts
- Aqua ducts

### Connecting infrastructure

- Tracks
- Tunnels
- Bridges/viaducts
- Switches/Rail junctions
- Highways
- Tunnels
- Bridges/viaducts
- Junctions
- Waterways
- Ship locks / lifts
- Aqua ducts

### Nodes (transaction point)

- Cargo terminal
- Rail marshalling yards
- * Logistic terminal
- * Inland ports/terminals
- * Ports/Terminals

### Control Systems

- * Central Rail Traffic Management
- * Local Rail Traffic Management
- * Road traffic management systems
- * Vessel traffic management
- * Traffic signs
- * Vessel traffic management

### Communication Systems

- * Communications network
- * Communications network / mobile network
- * GPS/VHF/AIS network
- * GPS/VHF/AIS network

### Power supply

- * Cateranies
- * Power supply national grid
- * Diesel stations
- n/a (self powered vehicles)
- n/a (self powered vessels)
- n/a (self powered vessels)

### Staff

- * Driving personnel
- * Handling personnel
- * Maintenance personnel
- * Information processing personnel
- * Driving personnel
- * Handling personnel
- * Maintenance personnel
- * Information processing personnel
- * Driving personnel
- * Handling personnel
- * Maintenance personnel
- * Information processing personnel

### Mobile units

- * Locomotives
- * Trucks
- * Vessels
- * Vessels
- * Rolling stock
- * Trailers
- * Barges
- n/a

### Cargo

- * Non-dangerous
- * Explosive
- * Toxic
- * Flammable
- * Non-dangerous
- * Explosive
- * Toxic
- * Flammable
- * Non-dangerous
- * Explosive
- * Toxic
- * Flammable

To avoid the inclusion of irrelevant detail road traffic lights and traffic signs and shipping buoys have not been included as transport elements which can be subjected to terrorist interventions.

### 2.2.2 Terrorist intervention methods

The terrorist intervention scenarios are identified based on a number of standard possible terrorist intervention methods. These intervention methods describe the possible attacks of which history has shown that they can be used by terrorists. Figure 2.3 gives an overview of the identified intervention methods and a brief description.

<table>
<thead>
<tr>
<th>Terrorist intervention methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Incendiary/fire</td>
<td>Arson using incendiary devices</td>
</tr>
<tr>
<td>2. Explosion: Detonation charge &lt;~30 kg TNT or eqv</td>
<td>Small charges transportable with back-packs to initiate larger explosions</td>
</tr>
<tr>
<td>3. Explosion: ~ 30kg TNT or eqv.</td>
<td>Charges transportable with small vehicles</td>
</tr>
<tr>
<td>4. Explosion: ~ 3.000kg TNT or eqv.</td>
<td>Charges transportable with larger road vehicles such as lorries</td>
</tr>
<tr>
<td>5. Poison attack</td>
<td>Dispersion/release of poison</td>
</tr>
<tr>
<td>6. Biological/ biochemical/chemical attack</td>
<td>Dispersion/release of biological/(Bio)chemical agents</td>
</tr>
<tr>
<td>7. Terrorist threat</td>
<td>An attack threat such as a bomb alert</td>
</tr>
<tr>
<td>8. Nuclear</td>
<td>Nuclear device resulting in nuclear explosion</td>
</tr>
<tr>
<td>9. Nuclear Dust</td>
<td>Dirty bomb resulting in nuclear radiation</td>
</tr>
<tr>
<td>10. Hijacking</td>
<td>Taking control using force, misuse, abuse or infiltrate</td>
</tr>
<tr>
<td>11. Mechanical/ Physical intervention</td>
<td>Sabotage or physical obstruction</td>
</tr>
<tr>
<td>12. Electronic attack (cyber crime)</td>
<td>Hacking or disruption of computer systems or electronics</td>
</tr>
</tbody>
</table>

Figure 2.3: Terrorist intervention methods
For explosives three subcategories have been created to differentiate in size and the possible ways to get them on the selected target location. The detonation charges are minor explosions applicable for setting of larger explosions in for example explosive cargo. The explosives of 30 kg TNT or eqv. are transportable by person or using small road vehicles. The explosives of 3000 kg TNT or eqv. are transportable using large road vehicles such as lorries.

2.2.3 Terrorist Intervention Database

For each of the elements identified in figure 2.2 the terrorist intervention methods, as identified in figure 2.3, are applied to define the possible terrorist intervention scenarios.

In each scenario a distinction is made between the direct consequences and possible sequential consequences. Direct consequences are fatalities and down time directly incurred by the attack on the specific transport element. Sequential consequences are fatalities and down time incurred in other elements as a result of such attack.

In total 221 terrorist intervention scenarios have been identified and analysed for the various transport elements. These scenarios can be combined to create larger sequences of events.

2.3 Transport security risks

From the comprehensive overview of the quantified terrorist intervention scenarios, as recorded in the terrorist intervention database, the transport security risks can be deduced. These risks can be classified into two categories.

1. **Infrastructure risks**: The terrorist has the objective to damage or destroy transport elements in order to disrupt the transport supply chain. The transport elements are in this case the terrorist’s target and can be found in scenarios with high direct consequences in terms of down time. The database has shown that these “target” scenarios are generally linked to infrastructure elements and will therefore be referred to as infrastructure risks.

2. **Supply chain risks**: The terrorist has the objective to misuse the transport supply chain as their means to create damage or fatalities. The transport elements are in this case not the target but the means and can be found in scenarios with high sequential consequences. The database has shown that the misuse of the supply chain can be linked to four basic scenarios to which the transport elements can be related:
   - The transport supply chain is misused as means of transport
     - i. The mobile unit or cargo is used as a means to conceal and transport various explosives, incendiary devices or nuclear devices to a location where they are unloaded or detonated.
   - The transport supply chain is misused as a weapon
     - ii. The cargo is used as a weapon: Release of dangerous goods such as toxic or biochemical cargo in preferably densely populated areas.
     - iii. The cargo is used as a weapon: Detonation of dangerous goods such as flammable and explosive cargo in preferably densely populated areas.
     - iv. The mobile unit is used as a weapon: Collision of the mobile unit using its physical characteristics to cause damage to infrastructure or fatalities or indirectly by colliding with another mobile unit which contains dangerous goods to create a release or an explosion.
2.3.1 Infrastructure risks

In the terrorist intervention database 51 confidential scenarios are identified with a high risk level. These scenarios received a red risk score according to the security risk matrix for their direct consequences. Each of these scenarios is directly linked to a transport element which can be considered the terrorist’s target. Based on these high risk scenarios, ten critical types of infrastructure elements are identified:

1. Rail/Road tunnels
2. Rail/Road bridges
3. Multimodal terminals
4. Logistics terminals (Rail & Road)
5. Ports/Terminals (Inland and short sea shipping)
6. Rail marshalling yards
7. Central Rail Traffic management systems
8. Power supplies to rail systems
9. Waterways
10. Ships locks

Consequences: Economic impact

The economic impact of the scenarios in the terrorist intervention database have been expressed in terms of expected down time based on a generic analysis of a possible worst case. However, further analysis of the potential economical effects in terms of financial costs needed to be made.

Terrorist interventions to transport infrastructure impact transport flows causing a disruption in a transport link or whole transport corridor simultaneously resulting in detours, delays and modal shifts. The economic cost of such a disruption is calculated in terms of extra transport cost and the necessary reconstruction cost. The extra transport cost is dependent on, among others, the volume and type of cargo passing the infrastructure, the by-pass capacity, availability of alternative modes and the expected down times. Accordingly the transport cost and thus the potential economical cost of a terrorist intervention on a critical transport element is very much so dependent on the specific location of the element in the transport infrastructure network (figure 2.5) and the distribution of the transport flows over this network.

Figure 2.5: Transport infrastructure network
The distribution of the trade flows, respectively transport demand to the transport infrastructure network (transport supply) was carried out by means of simulations in the European Freight Model (EFM). The transport patterns in the model result from simulations and illustrate the most cost and time efficient mode and route choice for freight flows.

To calculate potential economic cost of a terrorist intervention, 10 main corridors for international freight transports within the EU 25 have been identified based on selected criteria.

- Transport volume
- Potential presence of critical elements
- Possible high down times
- Difficulty of rerouting
- Presence of industrial and urban population
- Geographical coverage

Critical infrastructure elements along these 10 corridors have been identified and assessed in order to find the most vulnerable potential targets within the transport infrastructure network for international freight transports in Europe. Subsequently the effects of a potential terrorist intervention on the critical infrastructure along the tested main freight corridors have been estimated and quantified in a model environment by means of freight flow simulations with the EFM STAN model and scenario techniques.

From a confidential scenario analysis covering the 10 corridors, it can be concluded that a terrorist intervention on the most critical transportation corridor including the reconstruction times and cost to restore the full capacity of the link, the economic damage could tally up as high as 6.6 Billion Euros. These are only the direct economic costs of the disruption of a single link or corridor. It does not take account of any indirect costs due to damage to surrounding areas, fatalities or economic instability caused by the attack. (For reference: Economic cost to the Italian economy alone because of the Mont Blanc fire have been estimated at 0.5 B€ per year)

The assessment has also shown that critical corridors, those with highest impact on EU economy if disrupted, combine the following constellation of indicators:

- high transport volumes;
- limited number of competitive by-pass capacity;
- limited availability of competitive mode alternatives;
- infrastructure elements with long (re-)construction periods;
- infrastructure elements with high reconstruction costs; and
- high share of transport cost sensitive commodities.

2.3.2 Supply chain risks
The supply chain risks refer to the risk of misuse of the supply chain by the terrorist as their means to create damage or inflict casualties. The transport system is in this case not the target but the means. Two types of misuses have been identified. The supply chain can either be misused as a means of transport for malicious cargo or as a weapon where the inherent haz-
ard of the supply chain is released (e.g. release of toxic cargo, explosion of explosive cargo). Each type of supply chain risk is discussed separately below.

**Supply chain is misused as a means of transport**

Cargo is transported all throughout Europe, by trucks, trains or vessels. The content of cargo varies from raw materials to finished consumer products, travelling from production centres to other production centres or to the final consumer and passing key areas such as industrial locations and densely populated areas.

Both the cargo and the transportation units are ideal means to conceal and transport terrorist’s malicious goods such as explosives or other devices to locations where they can be unloaded or detonated. These locations can either be infrastructure elements in the transport supply chain, in which case the supply chain is misused to disrupt the supply chain, or locations such as industrial and populated areas to damage the economy and create fatalities.

The risk assessment study has shown a number of confidential scenarios are not unlikely to occur. However, it is not difficult to imagine that the most significant object to conceal in cargo or the transportation units to be transported by the supply chain is a nuclear or bio-terrorist device. The cost of a nuclear or bio-terrorist attack on the freight transport system and supply chain will have broad ranging and significant negative impact going beyond the transport system itself but also affecting adjunct and supporting activities.

Previous studies by Abt Associates Inc. calculated the economic impact of a single nuclear attack on a major US seaport and the impact of a bio-terrorist attack on the freight transport system with the following results:

<table>
<thead>
<tr>
<th></th>
<th>Nuclear attack</th>
<th>Bio-terrorist attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatalities</td>
<td>50,000 to 1,000,000</td>
<td>30,000 to 3,000,000</td>
</tr>
<tr>
<td>Property damage</td>
<td>$50 to $500 Billion</td>
<td>$1 to $10 Billion</td>
</tr>
<tr>
<td>Direct disruption to trade</td>
<td>$100 to $200 Billion</td>
<td>$20 to $200 Billion</td>
</tr>
</tbody>
</table>

Similar impact is possible to major European cities.

While concealment of a nuclear device in cargo is not unrealistic, at present there is no proof of any terrorist organisation having nuclear capabilities. There are however rumours and suspicions of possible missing nuclear devices in the former Soviet Union and the possible consequences of nuclear programs of countries such as Iran and North Korea.

Far easier and within the capacity of terrorist organisations is the concealment of multitudes of smaller explosives in the supply chain, as described in the possible scenarios above. Through easy access at transfer points, such as loading and storage facilities, when the cargo is not moving or through infiltration of supply chain organisations, terrorists can easily conceal many explosives. Through random detonation explosions may occur at critical infrastructures, transfer points, distribution centres, industrial areas, populated areas, dense traffic etc. Furthermore the supply chain will grind to a halt to allow inspection of all cargo.

**Supply chain is misused as a weapon**

When the supply chain is misused as a weapon the terrorist utilises high inherent hazard in specifically dangerous cargo to cause massive devastation, either in terms of fatalities or as damage to the economy. The consequences will be substantially larger than the terrorist inter-
vention itself, because with simple interventions terrorists can possibly release the great potential hazards of the dangerous goods.

From the terrorist’s point of view, dangerous goods are interesting targets because they are “free”, as they do not need be specially acquired, produced and carried, they pass many vulnerable locations (e.g. main stations, densely populated areas, tunnels and bridges) and they are easily identifiable because of clear marking on the transportation means.

Two identified types of misuse of dangerous goods are the release of toxic cargo or the detonation of explosive cargo. The risk assessment study has identified a number of confidential scenarios for the misuse of he supply chain. Based on those identified scenario’s, a quantitative analysis has shown that the explosion of 40 tonnes of LPG (slightly larger one containment unit for road and rail) would cause structural damage and fatalities within 150m, likely to cause fatalities among people outside within 300m and would inflict injuries within 500m.

A second analysis has shown that the instantaneous release of 1000kg of Chlorine would inflict 250 fatalities (assuming density of 200 persons per hectare) with no wind. If there is wind, the chlorine will disperse and could inflict thousands of fatalities.

Historic references to support the above calculations. The tragedy at Bhopal in India where methyl isocyanate leaked from a tank resulted in almost 4000 deaths. While a propylene explosion in a road tanker near a campground in San Carlos, Spain on 11 July 1978 resulted in 217 fatalities.

2.4 Risk to Europe

Based on the above considerations and the terrorist intervention database, European freight transport and its supporting supply chains can be considered at considerable risk to terrorist interventions.

Economic consequences

The consequences of a possible terrorist intervention on the supply chain itself can result in billions of Euros economic damage to the EU. While the misuse of the supply chain as transportation means for a weapon of mass destruction such as a nuclear device would be the ultimate doom scenario with unthinkable damage to the economy through the destruction of a whole city.

Fatalities

A misuse of the supply chain as weapon could result in possible thousands of injuries and fatalities. While here also the misuse of the supply chain as concealment and transportation means for a nuclear device would be the ultimate doom scenarios. Fatalities in major cities would be in the hundreds of thousands.

Vulnerability

The vulnerability of the supply chain to terrorist interventions can be considered high. Especially misuse of the supply chain as weapon requires minimal interventions to create maximum effect.
3.0 Mitigating the risk to infrastructure

This part of the report addresses securing the infrastructure and formulates mitigation measures which contribute to securing the transport infrastructure against terrorist interventions which have the objective to disrupt the transport supply chain. The intermodal transport network is in this case the target, instead of the means.

3.1 Vulnerability of and mitigation measures for the infrastructure

The critical types of infrastructure elements, as identified in section 2.3.1. above, have been assessed to determine the measures necessary to mitigate the risks which the risk assessment singles out as being imminent.

For these 10 types of critical infrastructural elements 20 generic mitigation measures have been defined and their applicability to each of the 10 types has been determined. These mitigation measures vary considerably in costs and effectiveness. To assist in identifying the most effective mitigation techniques the measures have been grouped in the most commonly deployed order in terms of effectiveness at various types of transport infrastructure.

<table>
<thead>
<tr>
<th>Mitigation Measure</th>
<th>Rail &amp; Road Tunnels</th>
<th>Road &amp; Rail Bridges</th>
<th>Multi Modal Terminals</th>
<th>Rail Marshalling Yards</th>
<th>Rail CRT Management</th>
<th>Logistics Terminals Road</th>
<th>Waterways</th>
<th>Ship Locks</th>
<th>Terminals - Short Sea</th>
<th>Power Supply</th>
<th>Rail Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>M03 - Perimeter Fencing Standard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M08 - Access Control Manual</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M06 - Security Lighting</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M01 - CCTV Manual</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M05 - Portal Protection Automated</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M02 - CCTV Motion Detection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M07 - PIDS Motion Detectors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M14 - Hazchem Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M17 - Security Awareness/Exercise Program</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M20 - Computer Security Measures</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>M04 - Perimeter Fencing Alarmed</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M09 - Access Control System - Automated</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 - Traffic Inspection Manual</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M11 - Traffic Inspection - Explosive Detection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M15 - Risk Management System</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M16 - Staff Vetting &amp; Training</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M18 - Security Guard Force</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M13 - Breakdown Recovery</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M19 - Security Dogs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M12 - Traffic Inspection - X-Ray Screening</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: X = Most likely sites for deployment

Figure 3.1: Effectiveness of identified mitigation measures
3.2 Investments needed to secure the infrastructure

Based on the applicability of the mitigation measures cost bands are set up on minimum / maximum basis for both simple and complex variants of each infrastructure type.

<table>
<thead>
<tr>
<th></th>
<th>Minimum 1st year</th>
<th>Maximum 1st year</th>
<th>Minimum 2nd year</th>
<th>Maximum 2nd year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Rail/Road tunnels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>148,000</td>
<td>18,000</td>
<td>265,000</td>
<td>45,000</td>
</tr>
<tr>
<td>Complex</td>
<td>5,215,000</td>
<td>1,015,000</td>
<td>10,607,500</td>
<td>1,907,500</td>
</tr>
<tr>
<td>2. Rail/Road bridges</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>204,000</td>
<td>54,000</td>
<td>411,000</td>
<td>81,000</td>
</tr>
<tr>
<td>Complex</td>
<td>3,897,500</td>
<td>797,500</td>
<td>8,755,000</td>
<td>1,605,000</td>
</tr>
<tr>
<td>3. Multimodal terminals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>145,000</td>
<td>45,000</td>
<td>676,000</td>
<td>126,000</td>
</tr>
<tr>
<td>Complex</td>
<td>4,837,500</td>
<td>887,500</td>
<td>10,777,500</td>
<td>1,977,500</td>
</tr>
<tr>
<td>4. Rail marshalling yards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>116,000</td>
<td>36,000</td>
<td>530,000</td>
<td>86,000</td>
</tr>
<tr>
<td>Complex</td>
<td>4,042,500</td>
<td>842,500</td>
<td>9,562,500</td>
<td>1,862,500</td>
</tr>
<tr>
<td>5. Rail CRT Mgt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>373,000</td>
<td>153,000</td>
<td>1,696,000</td>
<td>396,000</td>
</tr>
<tr>
<td>Complex</td>
<td>4,117,500</td>
<td>687,500</td>
<td>8,117,500</td>
<td>1,517,500</td>
</tr>
<tr>
<td>6. Waterways</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>85,000</td>
<td>45,000</td>
<td>282,000</td>
<td>72,000</td>
</tr>
<tr>
<td>Complex</td>
<td>1,100,000</td>
<td>400,000</td>
<td>4,675,000</td>
<td>825,000</td>
</tr>
<tr>
<td>7. Ship locks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>143,000</td>
<td>63,000</td>
<td>557,000</td>
<td>117,000</td>
</tr>
<tr>
<td>Complex</td>
<td>3,072,500</td>
<td>622,500</td>
<td>7,395,000</td>
<td>1,345,000</td>
</tr>
<tr>
<td>8. Terminals (Short sea)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>373,000</td>
<td>153,000</td>
<td>1,696,000</td>
<td>396,000</td>
</tr>
<tr>
<td>Complex</td>
<td>3,847,500</td>
<td>687,500</td>
<td>8,117,500</td>
<td>1,517,500</td>
</tr>
<tr>
<td>9. Power supply to rail</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple</td>
<td>114,000</td>
<td>54,000</td>
<td>411,000</td>
<td>81,000</td>
</tr>
<tr>
<td>Complex</td>
<td>2,327,500</td>
<td>577,500</td>
<td>6,715,000</td>
<td>1,215,000</td>
</tr>
</tbody>
</table>

Figure 3.2: Cost bands for each infrastructure type

An analysis has been made of the maximum investment required to protect the main cargo traffic corridors in Europe. These investments are less than 0,5% of the potential economic damage which could be caused by terrorists succeeding to obstruct these corridors by destruction. Only securing the Pan-Alpine crossing would require a higher investment, namely 1.30%.

It can be concluded that the cost of investing in a full range of mitigation measures is extremely low compared to the possible economic costs of a potential terrorist intervention.

The delays caused by mitigation measures such as cargo scanning and the subsequent economic cost have been determined to be insignificant based on experience at the Eurotunnel.

3.3 The vulnerability assessment tool

Part of the deliverables of the study has been a “Vulnerability Assessment Tool”, i.e. a checklist through which the owners of infrastructural elements can make an assessment of the vulnerability of the individual elements to provide a basis for prioritising investments in securing the infrastructure. See Appendix A.

3.4 A sample security plan to protect infrastructure

Similarly a draft template for a “Security Plan to Protect Infrastructure” has been developed which can be utilised by owners of infrastructural elements to take a harmonised approach to managing the security of their assets. See Appendix B.
4.0 Mitigating the risk to the supply chain

Whereas the previous chapter focused on securing the infrastructure as a target of terrorist interventions, the focus of this chapter is on securing the supply chain against misuse by terrorists as their means to create damage or casualties. Four types of misuse have been defined:

1. The mobile unit or cargo is used as a means to transport various explosives, incendiary devices or nuclear devices to a location where they are unloaded or detonated.
2. The cargo is used as a weapon: Release of dangerous goods such as toxic or biochemical cargo in preferably densely populated areas.
3. The cargo is used as a weapon: Detonation of dangerous goods such as flammable and explosive cargo in preferably densely populated areas.
4. The mobile unit is used as a weapon: Collision of the mobile unit using physical characteristics to cause damage to infrastructure or fatalities or indirectly by colliding with another mobile unit which contains dangerous goods to create a release or an explosion.

4.1 Approach

The inventory of security risks which provided a comprehensive and holistic overview of the potential terrorist interventions in the intra EU supply chains forms the basis for the development of the measures and instruments required for improving the security of the supply chain.

4.1.1 Event trees

For all four transport modes (rail, road, inland waterways and short sea shipping) and for each of the four above identified scenarios event trees are developed. Using the event trees the scenarios can be traced back to a large variety of initial interventions/events and corresponding root causes (requirements), which initiate the materialisation of any of these misuse scenarios.

4.1.2 Root causes

Since different branches on event trees can be traced back to similar root causes, there exists the need to summarise and categorise the identified root causes to determine the distinct root causes. Categorisation of the root causes takes place on the three axes representing the three elements of the supply chain which are presented in figure 4.1.

1. Transport mode.
   a. Road.
   b. Rail.
   c. Inland waterways.
   d. Short sea shipping.
2. Supply chain process.
   a. Before taking into use.
   b. Loading.
   c. Storage.
   d. Transportation.
   e. Information.
   a. Infrastructure.
   b. Operational elements.
   c. Cargo.
4.1.3 Defining mitigation measures

Mitigation measures are identified per distinct root cause. Since one distinct root cause can contribute to one or more branches in the event tree, the possible different initial events resulting from one root cause are defined.

Example:
For the root cause “access to trucks/trailers at maintenance areas”, two initiating events can be identified using the event trees
1. Sabotage of truck/trailer at maintenance area
2. Placement of charges in confined spaces of trucks/trailers by terrorist during maintenance

Accordingly for each possible initial event, through qualitative assessment, mitigation measures are specified. Mitigation measures in this context are interventions which either
- Reduce the likelihood of the materialisation of the initiating event or
- Limit the consequences of the initiating event.

Only those mitigation measures have been further considered which reduce or contribute to the reduction of the risk as defined in the security risk matrix, figure 2.1, from red or yellow to green. Measures which are impossible to realise (for example physical access control to highways and railways by completely fencing off the infrastructure) are also not considered.

Example:
For the first initiating event from the example case, sabotage of truck/trailer at the maintenance area, the following mitigation measures have been defined:
1. Deny unauthorised access to other persons than own or subcontractor staff.
2. Ensure that persons, other than own or subcontractor’s staff are always accompanied by a trusted person.
3. Ensure that vehicles are thoroughly inspected upon (re)delivery by driver.

For each mitigation measure a first qualitative assessment is made of its feasibility. The feasibility of a measure is determined using two factors, each ranked on a scale 1 to 5:
- Ease of implementation: an assessment of the implementation of the measure based on a qualitative analysis of factors such as costs, time and the operational framework.
- Effectiveness: an assessment of the expected impact of the measure on the reduction of the likelihood or the consequences.

The feasibility score is ranked into three main categories according to the matrix in figure 4.2.
1. Red: Very low feasibility (score 1 to 4) and low feasibility (score of 5 to 7)
2. Yellow: Medium feasibility (score of 8 to 14)
3. Green: High feasibility (score of 15 to 19) and very high feasibility (score of 20 to 25)

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of implementation</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Figure 4.2: Feasibility scoring matrix
For each feasibility analysis a qualitative consideration is given to the operational framework / working environment in which each distinct root cause normally takes place. This gives insight into any typicality’s and specific characteristics of the root cause as a step in the whole supply chain. On the one hand it calibrates the relevance of the reviewed events while on the other hand supports the feasibility assessment of each mitigation measure. Feasibility of a mitigation measure is mainly determined by the operational framework in which it must operate.

**Example:***

The following operational framework description has been given for the distinct root cause from the example case:

For road vehicles there exists a wide variety of repair and maintenance facilities, ranging from service garages, body repair workshops, painting companies, tire centres etc. The total number of these facilities within the EU is estimated to be in the order of 20,000. The typical characteristics of these organisations are that: they differ largely in size, ranging from mid size, well structured organisations down to one or two man operations. Besides they are (and to some extent need to be) easily accessible to the public. Truck drivers, maintenance personnel for service equipment and other people who are not under control of the organisation have access to the premises and the vehicle.

Where appropriate, similar mitigation measures for similar root causes in different modes or for different types of root causes within one mode have been grouped logically into one potential measure in a final summary of possible mitigation measures.

### 4.2 Generic overview of mitigation measures

Based on the final summary of mitigation measures a distinction is made between minimum mitigation measures applicable at all times and mitigation measures only applicable during heightened security threat.

**Security threat levels**

There exists a direct relationship between the security threat, generally expressed in predefined security threat levels, and the extensiveness of implementation of mitigation measures. The higher the threat of an expected terrorist attack, the more extensive the implemented mitigation measures.

An example of a security threat level system is defined in the ISPS code as adopted by the IMO:

- **Security Level 1**: normal, minimum appropriate protective security measures shall be maintained at all times.
- **Security Level 2**: heightened, appropriate protective security measures shall be maintained for a period of time as result of heightened risk for a security incident.
- **Security Level 3**: exceptional, further specific protective security measures, as defined by the appropriate authorities, shall be maintained for a period of time when a security incident is probable or imminent.

Such three tiered approach can very well work in defining protective measures for the transportation infrastructure. Considering the large number of organisations that are affected by supply chain security requirements the introduction of a three tiered system seems to be impractical. It is difficult to envisage that an economic system with so many operators can effectively adjust its operational procedures and security measures from level 1 to level 2 or 3. It is, therefore, suggested that the selected minimum protective mitigation measures in the supply chain already provide a fairly high level of security at normal operations. Only when indications exist that a security incident is probable or imminent, further specific protective security measures, as defined by the appropriate authorities, shall be maintained for designated operators over a specified period of time and in a specified area or field of work. This two tiered approach is supported by the International Chamber of Commerce during the work on security standards within the security taskforce of the WCO.
4.2.1 Minimum mitigation measures

Based on the analyses as described in 4.1 above the following, feasible and effective generic mitigation measures have been defined.

A. Mitigation measures to be taken by all
   1. Security risk assessment
   3. Deny unauthorised access to the organisation.
   4. Deny unauthorised access to critical working areas.
   5. Implement training and awareness programs.
   6. Prevent use of bogus sub-contractors.

B. Mitigation measures to be taken where appropriate
   7. Deny unauthorised access to means of transport (transportation).
   8. Deny unauthorised access to cargo (loading, storage or transportation).
  10. Deny unauthorised access to steering houses in means of transport (transportation).
  11. Deny unauthorised access to traffic control systems (transportation).
  12. Deny unauthorised access to cargo and transport information (information handling).
  13. Inspect confined spaces in the means of transport and cargo (loading or transportation).
  14. Separate dangerous goods from other cargo (loading, storage or transportation).
  15. Reroute dangerous cargo (loading, storage or transportation).

These generic mitigation measures are considered in more detail below.

A. Mitigation measures to be taken by all

Ad 1: Security risk assessment
Since operations and companies may have a nature, size and operational environment which varies enormously a set of minimum mitigation measures cannot be taken for granted as being most effective. Companies must make an assessment of the risk to their own operations and take those measures that mitigate those risks in the most effective matter, suiting the type and size of the operation.

A company risk assessment must take account of the possible terrorist threats it is subjected to, the possible consequences of a successful attack, the vulnerabilities of the company regarding terrorist threats and the impact of the company characteristics on the effectiveness of possible mitigation measures.

Ad 2: Security mindset
Success of terrorist security programs depend on the awareness of the company and its personnel. Only when the mind set of top management is focused on security, can the organisation become aware of possible terrorist threats and is successful implementation of the selected mitigation measures possible.

Ad 3: Deny unauthorised access to the organisation
Unauthorised access by a terrorist to an operator’s organisation can be achieved by infiltrating the organisation as a permanent or temporary staff member. While performing regular staff duties the terrorist has access to the supply chain and can misuse it to his advantage. Threat of infiltration is applicable to all operators in the supply chain. Security background checks of em-
ployees, better known as vetting, may be an effective measure to prevent infiltration of terrorists in the organisation. However, ease of implementation of such a mitigation measure is dependent on the mobility of the employees, which refers to the stability of the work relationship. In the transport supply chain three main categories are identified:

- Low mobility: employees have stable work relationships and stay with one employer for longer periods of time. Outsourcing is limited to a small number of sub-contractors.
  - Maintenance & transportation organisations in the rail sector.
  - Transportation organisations inland shipping.
  - Supervisory staff in all organisations.

- Medium mobility: employees have a reasonable stable work relationship and movement of employees between employers occurs occasionally. Regular outsourcing of work.
  - Maintenance organisation in the road sector.
  - Transportation organisation in short sea shipping.

- High mobility: employees have unstable work relationships and movement of employees between employers occurs regularly. Outsourcing of work is very common.
  - Loading and storage organisations in all transportation modes.
  - Transportation organisations in the road sector.
  - Maintenance organisations in the inland and short sea shipping sector.

Implementation of employee vetting in organisations with low employee mobility is easily executable by the employers, because of the low number of screenings required to be performed annually. However, as mobility of employees increases the implementation becomes more difficult, while the effort required for sustaining an effective program increases. For organisations such as loading, storage and maintenance organisations in the shipping sectors employee vetting could be implemented only for supervisory staffs, who oversee activities performed by unvetted staff. This will not be possible for transportation organisations and therefore, special attention will need to be paid to vetting of drivers in the road sector when developing the required instruments for employee vetting.

Ad 4: Deny unauthorised access to critical working areas

Critical working areas are identified for each of the supply chain process steps. A number of these working areas characterise themselves as closed systems. They can be warehouses, indoor workshops, offices, or securely fenced off outside areas. In general there are only a limited number of entry points to the working area and restricted third party involvement. Critical working areas operating as closed systems include:

- Rail maintenance workshops (before taking into use).
- Loading areas for rail, inland and short sea shipping (loading).
- Storage areas for all transport modes (storage).
- Rail traffic control centres (transportation).
- Short sea ports (generally an ISPS port and therefore a closed system) (transportation).
- Information processing areas (information).

Entry and access to these critical working areas is controlled and therefore the denial of unauthorised access is easily achieved with technical and procedural measures. Proposed measures in the IMF matrices include:

- Access procedures.
- Ensure fencing, locking devices, entrances etc are properly maintained.
• Challenge unknown persons to reveal their identity and justify their presence.
• Use of Closed Camera TV systems (CCTV).
• Critical areas have both inside and outside adequate lighting.

Other critical working areas do not function as closed systems and are separately discussed below:

• **Truck and ship maintenance/repair yards** (before taking into use): Due to their open nature, preventing unauthorised access to the facilities is extremely difficult, if not impossible. Therefore, the only realistic mitigation measures for these companies are:
  - Inspection of confined spaces in trucks/trailers by the truck driver before leaving the workshop.
  - Inspection of confined spaces in barges and vessels by inspection/ supervisory staff from the yard and/or the crew before leaving the yard.
  - Vetting of truck drivers, ships crew members and inspection/ supervisory staff of shipyards.

• **Road loading areas** (loading): Due to their open nature, often easily accessible load bays especially for the smaller sized production organisations/manufacturers, measures to deny unauthorised access are more difficult to implement than for the other three sectors. Therefore, for these types of companies more emphasis needs to be on:
  - Deny unauthorised access to the cargo through continuous supervision of loading operations by a trusted employee.
  - Inspect cargo containments before loading.

• **Parking places** (transportation): Considering the public characteristic and quantity of parking places it is impossible to deny unauthorised access and to realise measures such as fencing, lighting and CCTV for all areas. Focus will need to be on:
  - Denying unauthorised access to cargo and means of transport.
  - Inspection confined spaces in trucks/trailers before leaving area.
  - Further elaboration of the number of secure parking areas, such as identified by the IRU and ECMT in their list of Truck Parking Areas in Europe 2003, which can be utilised by trucks transporting high vulnerability cargo.

• **Marshalling yards** (transportation): Are large open areas and therefore difficult to secure. While some achievements can be made with support of CCTV systems and surveillance. Focus should, like in the parking places, be on:
  - Denying unauthorised access to cargo and means of transport.
  - Inspection confined spaces in rolling stock before leaving area.

• **Inland shipping dock sides** (transportation): At present an inland ship can stop/rest at any public dock along the waterway. These are open and public places for which the denial of unauthorised access is impossible. Measures can either focus on
  - Denying unauthorised access to the cargo and means of transport.
  - Setting up secure dock sides as closed systems where inland ships are required to berth.

• **Connecting infrastructure for all modes** (transportation): roads, rail tracks and waterways (incl. dikes) are impossible secure against unauthorised access. It is unrealistic to fence off or guard all connecting infrastructure. The focus should therefore be on:
  - Denying unauthorised access to cargo and means of transport.
  - Rerouting and flexible routing of dangerous cargo.

---

7 www.cemt.org/online/pubpdf.htm
Ad 5: Implement training and awareness programs
While employee vetting is an effective way to prevent suspected terrorists from infiltrating organisations, it does little against people with no suspicious or incorrect backgrounds, people who develop positive feelings towards terrorism only after having been employed or employees which have been blackmailed. Especially against blackmail there are no preventive measures which can be taken by operators.

To anticipate on this the main focus needs to be on training and awareness programs which help employees identify suspicious behaviour. It improves overall terrorist and security awareness in the organisation and it involves the employees directly in improving the security in the organisation.

Ad 6: Prevent use of bogus sub-contractors
Similar measures as those in place to prevent unauthorised access/infiltration in the organisation need to be in place to prevent the use of bogus sub-contractors. Only known sub-contractors shall be used and when engaging new sub-contractors these need to be vetted to identify any possible security threats.

Of particular interests are bogus sub-contractors in the maintenance/before taking into use phase and the transportation phase. During maintenance, especially in the shipping sectors, sub-contractors are widely used. Illegitimate sub-contractors have easy access to the transportation means and can easily sabotage or place explosives in confined spaces. During transportation, especially in the road sector, transport orders are often subcontracted to free lance drivers or third party drivers. The subcontracting of for instance a dangerous goods transport order to an illegitimate sub-contractor allows easy misuse of the supply chain as a weapon as the terrorist is given full control over the transport.

B. Mitigation measures to be taken where appropriate

Ad 7 Deny unauthorised access to means of transport
This measure is only applicable during the transportation phase of the supply chain and thus only needs to be implemented by transport operators. The denial of unauthorised access to the means of transport unfortunately, cannot be achieved through the denial of unauthorised access to the critical working areas and thus must be achieved at the means of transport itself.

For inland and short sea shipping the transportation means are small closed systems. Ships are physically protected by their hull, are easily observable by the bridge deck, have multiple crew members and when in transit on the waterway are difficult to approach. Denial of unauthorised access to the vessel can, therefore, be achieved through surveillance activities. Possible mitigation measures are:

- CCTV surveillance along the vessel’s hull.
- Ensure deck is lighted.
- Accompany non crew members whilst on board.
- Continual surveillance from the bridge deck.

For rail and road the transport means are open accessible structures and easy approachable, especially when stopped. Denial of unauthorised access to these means of transport can therefore not be achieved. The mitigation measures must therefore fully rely on:

- Deny unauthorised access to the cargo.
- Deny unauthorised access to the confined spaces in the means of transport.
• Deny unauthorised access to the steering houses.
• Inspection of cargo and transportation means during transport.

Ad 8: Deny unauthorised access to cargo
The mitigation measure is only applicable for the processes loading, storage and transportation. While it mitigates a wide range of interventions which lead up to a variety of misuses of the supply chain, two key critical interventions can be identified. The first intervention is the placement of large amounts of explosives or a nuclear device during the loading and storage processes to misuse the supply chain as transportation means. The second intervention is the misuse of dangerous goods as a weapon during transport.

The denial of unauthorised access to cargo during loading and storage is achieved through:
• Deny unauthorised access to the critical working areas (except for loading in transport mode road).
• Implement a seal and seal control program.
• Supervise loading operations.
• Ensure cargo complies with manifest and is collected by identified carrier.
• Inspect cargo containments before loading.

The denial of unauthorised access to cargo during transportation cannot be achieved through access control at the critical working areas since they are open and generally public places. While access denial of unauthorised access to the transportation means is only applicable for inland and short sea shipping. Identified measures to deny access to the cargo are:
• Where possible, stacking of containers door to door.
• No open dry bulk transports. Need to make use of tied-down tarp coverings which are secured, cable locked and sealed.
• Locking and sealing of general cargo containments (hard sided/top (container) and soft sided/top transports).
• Securing/locking and sealing of release points, valves and hatches on dangerous goods transports.
• Implementation of a seal and seal control program on all cargo holds and containments (soft sided/top, hard sided/top (container), dry bulk transports and dangerous goods transports).
• Ensuring keys are kept secure.
• Denial of unauthorised access to the transportation means (only applicable for inland and short sea shipping).

Cargo is, however, rarely continuously en route during the transportation phase. Regular stops are made by operators to load and unload, to rest or due to traffic situations. Stoppage is the time during transportation when the cargo is the most vulnerable to an intervention. On top of the measures taken to deny unauthorised access to the cargo extra measures need to be taken to enhance security during stoppage. Other measures need to focus on:
• Inspection of cargo and transportation means during transport after stoppage.

Remarks on seals and seal control programs
The application of seals and the implementation of a seal control program have two distinct functions. First of all, together with locks, they deny the unauthorised access to the cargo. While locks are often considered the first option, seals provide extra assurance in access control. However, more important is the second function of seals, which is the possibility to inspect
and verify if the cargo has been accessed by inspecting whether the seal has been tampered with.

The implementation of a seal control program concerns two aspects.

- First of all the EU should develop a seal program on the technical requirements of seals and the procedural requirements of operator seal programs. Indicating what seals must be applied when and where. Possible references for such a program are ISO PAS 17712, defining mechanical seal strength and operation, and the World Customs Organisation Seal Program. (More attention to this measure is paid in the chapter).
- Second, each operator must develop their own organisation seal program which meets the requirements set out in the EU seal program.

Ad 9: Deny unauthorised access to confined spaces in means of transport

This mitigation measure is only applicable during the transportation phase and shows many similarities to the denial of unauthorised access to cargo. Based on similar reasoning as for cargo, unauthorised access to the confined spaces cannot be achieved through denied access to the critical working areas or to the transportation means itself for rail and road transport. Mitigation must therefore focus on:

- All confined spaces, such as external storage compartments, are locked and secured at all times.
- Ensuring keys are kept secure.
- Denial of unauthorised access to the transportation means (only applicable for inland and short sea shipping).

However, due to the open physical structures of rail and road transport means it is impossible to completely secure the spaces in the means of transport. Especially during a stoppage is the vulnerability the greatest. Extra measures need to be taken to enhance security, focusing on:

- Inspection of cargo and transportation means during transport.

Ad 10: Deny unauthorised access to steering houses

In order to prevent hijacking of the transportation means during the transportation phase, unauthorised access to steering houses needs to be denied at all times. Steering houses form small closed systems on the means of transport and are with the help of technical and procedural measures easy to close off. Identified measures are:

- Keeping cabin/bridge doors locked at all times.
- Ensuring keys are kept secure.
- Passengers are not allowed in the cabin.
- Instalment of intrusion alarms.
- Denial of unauthorised access to the transportation means (only applicable for inland and short sea shipping).

Ad 11: Deny unauthorised access to rail traffic control systems

This measure is only applicable for the rail during the transportation phase. While access can be denied to the rail traffic control room/nerve centre (see deny access to critical working areas) it is nearly impossible to deny access to the control systems themselves. The control systems are the switches, cables running along the track, local switchboards, etc. They are easily accessed to be damaged or manipulated to cause collisions. Possible mitigation measure to compensate the easy access is:

- Training and awareness program for driving personnel to detect incorrect signalling.
Ad 12: Deny unauthorised access to cargo and transport information
Besides securing the information processing rooms, the information itself also requires to be secured against unauthorised access. Cargo and transport information is often passed from organisation to organisation through public communication channels or is stored in accessible locations. Identified mitigation measures in the IMF matrices:
- Secure computer systems against hacking.
- Ensure all documents are kept in a secured environment.
- Deny access of non-authorised personnel to this secure environment.
- Implement training and awareness programs on the importance of data security.

Ad 13: Inspect confined spaces in means of transport and cargo at appropriate moments
At certain moments in the supply chain the denial of unauthorised access is either not possible or does not provide sufficient security coverage. In support of the access control measures, inspection measures are required as suppressive mitigation to identify any suspicious activities or situations. Below the most key moments are discussed.

- **Before taking into use/after maintenance**: applicable for the transport modes road, inland and short sea shipping. For all three modes it was determined that the critical working areas could not be secured against unauthorised access, giving possible terrorists access to the means of transport to sabotage or place explosives in confined spaces. Therefore, it must be ensured that the transport means are thoroughly inspected upon redelivery to the supply chain. For road, the inspection can be performed by the driver, for shipping the inspection can be performed by the vetted supervisory staff.
- **Loading**: applicable for all transport modes. To ensure that unknown cargo does not get loaded together with known cargo, it must be inspected before being loaded into the cargo confinements. Special attention needs to be given to empty containments or containments which are assumed to be empty.
- **Transportation**: applicable for all transport modes. During transportation the transportation means and the cargo are the most vulnerable after having stopped and left unattended for a period of time. Even though cargo and confined spaces may be locked and possibly sealed this does not guarantee against an intervention and access to the cargo or confined spaces. After each stoppage where the cargo/transportation means are left unattended both need to be inspected to determine if any of the locks and seals have been breached to access the cargo or the confined spaces. This includes inspection of valves, hatches and release points for dangerous goods. Inspection is easiest to implement for trucks/trailers followed by the ships. For rail the measure is very difficult due to the length of the rolling stock and is therefore, under normal operation procedures, only recommended for dangerous goods.

Ad 14: Separate dangerous goods from other cargo
The misuse of the supply chain is often linked to an intervention to dangerous goods because of the inherent destructive potential of dangerous goods and the ease of the intervention. Direct explosions in the cargo are not always necessary to release the destructive potential. Explosions nearby or mechanical interventions such as opening valves or collisions are often enough. Direct access to the cargo is therefore not necessary, proximity is enough. For this reason dangerous goods require special but also stricter security measures than other cargo, especially if there is an imminent threat.
In order to effectively protect dangerous goods it is necessary to separate them from other cargo. The loading, storage and transportation needs to be done in specialised areas and transport means to allow effective mitigation measures to be implemented.

Ad 15: Reroute dangerous goods
To release the destructive potential of dangerous goods there is no need to have access to the cargo. Often an explosion nearby on the infrastructure or with use of a missile launcher would be sufficient. Considering the open structure of infrastructure but also the always present free line of sight to the means of transport and their cargo it is impossible to prevent both attacks.

However, to prevent such an attack being successful, timing and location of the dangerous goods transports must remain unknown. One aspect is denying unauthorised access to information about cargo and routes. A second aspect is keeping transport times and locations random by alternating schedules and routes, better known as flexible routing. A third option is to reroute dangerous goods transports away from densely populated areas and critical infrastructure to minimise the possible impact of the inherent destructive potential in the case the attack is successful.

Rerouting and flexible routing are most effective for road because of its densely available infrastructure network. For rail and inland shipping the measure is less effective because of the limited routing options.

4.2.2 Possible measures in case of imminent threats.
As mentioned before a two tiered security approach is suggested, differentiating between normal operations and situations where a security incident is probable or imminent. In case of probable or imminent security threats extra measures shall be defined by the designated authorities and shall be maintained by designated operators over a specified period of time and in a specified area or field of work, related to the identified threat. However, in section 1.5 it has been observed that presently many local authorities are not yet fully prepared for this task. Few countries work with threat level systems and have predefined measures linked to these levels.

The measures below are difficult to uphold for unlimited time and therefore have not been addressed in the previous section. However they are feasible for a specified period of time with extra effort are discussed below.

Deny unauthorised access to maintenance area for road and shipping
Under normal operations it has been determined that the maintenance areas for road, inland and short sea shipping are nearly impossible to permanently secure against unauthorised access because of their open structures and extensive use of subcontractors. Inspection schemes are applied to compensate for the possibility of an unauthorised access.

However, in case of probable or imminent threats aimed directly at the maintenance workshops the probability of an unauthorised access increases and with this the possibility of an intervention going unnoticed in the inspection scheme. Therefore, extra effort is required for the duration of the threat to secure the critical working areas in the affected geographic area against unauthorised access. Because of the characteristics of the organisations/critical working areas and the expected impact of the measures on normal operations, these measures can only be upheld for a short period of time. Possible mitigation measures can include:

- Where possible install (temporary) fencing.
- Ensure all locking devices, alarm systems and lightings are working properly.
• Strict access control procedures and surveillance.
• Only trusted staff and designated subcontractors are allowed on the premises. For road maintenance workshops even the driver delivers and picks up his vehicle outside the workshop premises. For shipping maintenance yard strict control must be enforced on the use of subcontractors.

Implement employee vetting for all personnel not just supervisory staff
For all loading and storage personnel and maintenance personnel working in the inland and short sea shipping sector it has been determined that due to the high mobility of the workforce the ease of implementing an employee vetting system for all employees is low and the effort required to sustain the system is high. During normal operations it has, therefore, been proposed only to vet all supervisory/inspection staff who oversee all activities performed by unvetted employees.

However, in case of a direct threat linked to infiltration of organisations, it is suggested that all personnel employed at that moment by any of the organisations in the geographic affected area are screened to have their backgrounds checked. The measure also needs to be applied to all new applicant employees for the duration that the threat exists. After the threat has ended the measure can be downgraded back to only vetting supervisory and inspection staff.

Only utilise well lit and fenced parking places for dangerous goods
Three key remarks were made in the previous section. First of all, parking places are critical areas which are impossible to secure against unauthorised access, because of their open and public character. Second, the cargo and transportation means are most vulnerable during stoppage in the transportation phase. Third, misuse of the supply chain as weapon is often linked to dangerous goods because of its inherent destructive potential and ease of intervention, with minimum delay between the intervention and the impact.

Therefore, when there are indications that a security incident is probable or imminent extra measures need to be taken to protect dangerous goods during stoppage at parking places. Even in case of imminent threats, due to sheer numbers and the public character it is still impossible to secure all parking places against unauthorised access. However, to provide a “safe haven” for dangerous goods transports two options exist:
• A limited number of parking areas along a number of international routes for dangerous goods are designated as secure parking areas for dangerous goods transports. They are fenced off, lighted and protected by surveillance teams. Drivers can reserve a parking place in such an area.
• Existing fenced and well lit parking areas such as properties belonging to transport, loading and storage operators are designated and temporarily used as “safe havens” while the threat exists. Where appropriate guards can be involved. Transport operators generally have large properties where they normally store all their trucks/trailers when not in use.

Deny access to marshalling yards through surveillance and fencing
Similar to parking places, marshalling yards cannot be protected against unauthorised access during normal operations. In case of heightened security threat marshalling yards will require intensive surveillance using CCTV and guards and fencing should be considered where possible which is determined by the size of the marshalling yard and the number of entry points. Especially the intensive surveillance is only possible for a limited time. Preference should be given to those marshalling yards which are located near densely populated areas and those harbouring dangerous goods.
Inspection of cargo for rail specifically for dangerous goods

While the means of transport and the cargo containments in the road sector are inspected each time they are left unattended during normal operations, for the rail sector this was not suggested because the length of rolling stock makes such a measure impracticable. It was therefore suggested that, during normal operations only dangerous goods cargoes are inspected in the rail sector. However, when a security attack is probable or imminent it is recommended that this measure is also implemented for all other cargo in the rail sector. For longer rolling stock the measure will require extra investments in staff to ride on the rolling stock and perform the inspections.

Strict implementation of seal/seal management program

Under normal operations a seal program is recommended only for cargo transports travelling multiple days. Based on the assumption that these transports will require stopping time where the means of transport and the cargo are left unattended. However, under increased threats of a terrorist incident the seal program can be temporarily expanded to cover all international cargo transports both one day and multiple days transport. This is based on the reasoning that all transports at one point will have to make unattended stops for refuelling or resting.

4.2.3 Contingency measures

The mitigation measures described in the previous section are all preventive measures aimed at preventing the occurrence of undesired events which can result in the misuse of the supply chain. Unfortunately 100% security does not exist and even with all mitigation measures implemented, the residual risk remains of a root cause materialising and an initiating event occurring. Therefore, with the knowledge of the security risks in the supply chain and the remaining residual risks, contingency plans need to be developed to deal with the occurrence of an undesir-able event.

An undesirable event in the supply chain can take on many different forms which have been discussed in great detail in the event trees in section 4.1.1. Examples of undesirable events can range from the beginning of the event tree, such as root causes/initiating events:

- Infiltration or blackmailing to control an organisation.
- Access to critical working areas resulting in sabotage/placement of explosives.
- Access to cargo to sabotage/place explosives.
- Etc.

To the end of the event tree such as the misuses of the supply chain themselves:

- Explosion due to explosives in cargo.
- Explosion of explosive dangerous goods.
- Release of toxic dangerous goods.
- Collision of the means of transport.

Responsibilities can be assigned to two main parties. On the one hand the responsibilities of the industry as operators in the supply chain and on the other hand the responsibilities of the local and national authorities as being responsible for coordination national crisis management and disaster recovery.

4.2.3.1 Industry

When an undesirable event occurs in the transport supply chain the operators in the supply chain are often the first line of interaction with that undesirable event. They are generally the first to identify the undesirable event and also the first party to act/react to the event. Contin-
Emergency planning must therefore be an integrated part of the total security plan for an operator. Incorporating procedures on what to do, how to act, and who to contact. Five key elements needed to be included in the operator’s contingency planning:

1. **Identification of an undesirable event**: If no party observes the undesirable event it is not known to have occurred and therefore no contingency measures can be taken. When it concerns exploding cargo or colliding means of transport identification is not difficult. However, identification becomes more difficult when the event is access to cargo or even infiltration into the organisation. Therefore, procedures/measures need to be formulated and training needs to be given on how to detect certain events such as infiltration in the organisation and access to cargo.

   Measures to identify undesirable events are closely linked to suppressive mitigation measures described in the previous section, such as training on how to identify suspicious behaviour, the implementation of a seal program and inspection activities.

2. **Actions after an undesirable event**: After an undesirable event has been observed the operator is the first line of interaction with that event. Emergency plans need to be developed describing the required action by the operator for each possible undesirable event within the work scope of the operator. Furthermore crisis management rooms need to be assigned from where the actions can be coordinated if necessary. For undesirable events such as the explosion or release of dangerous goods procedures can be extensive with a focus on first relief to minimise the impact of the event on fatalities and the consequences to the business. After which assistance is given to authorities in further disaster recovery. For other undesirable events such as infiltration into the organisation or blackmail there aren't many actions an operator can take, besides contacting the authorities.

3. **Interactions with authorities**: Each operator must know their contact persons at the local authorities and be able to contact them at any moment of time. Procedures need to be formulated describing who and when to contact in case of an undesired event.

4. **Training and testing**: The developed identification measures and emergency plans must be tested and trained periodically to determine their effectiveness and to improve the skills of the involved personnel in reacting to an undesired event.

5. **Prevention of reoccurrence**: If an undesired event has occurred lessons need to be learned to determine where and why the mitigation measures failed and how mitigation measures can be improved to prevent reoccurrence. The contingency planning therefore needs to include procedures on incident investigation and cause analysis.

4.2.3.2 Local and national authorities

Local and national authorities are responsible for the coordination of all national crisis management and disaster recovery activities. These activities come into force once an undesired event is identified and reported to the authorities. The procedures for these activities include advance planning and process establishment to operate in extraordinary circumstances and are incorporated into national contingency plans.

As determined in report 2, most EU Member States have implemented contingency plans. However, each Member State must determine how the existing contingency plans meet the
needs of and deal with the contingency measures required for undesired terrorist events in the
transport supply chain. National contingency plans must be well developed to deal with both:

1. Large incidents such as e.g. explosions and release of toxic goods; and
2. Small incidents such as e.g. the infiltration of organisations.

4.3 Current initiatives
It is imperative that new legislations which are being developed to improve security of the sup-
ply chain within the EU connects, where possible seamlessly, with existing initiatives or initia-
tives in progress to prevent duplication of efforts and cost escalating effects for trade and in-
dustry.

Airborne and maritime transport have established security regimes and also the transportation
of dangerous goods has become subject to security requirements since the beginning of 2005.

Traditionally, security Management of the land based supply chain only addressed the preven-
tion of theft and damage of cargo. An example of this is the certification program that has been
developed by TAPA (Technology Asset Protection Association). The attack on the WTC on
September 11 2001, however, has increased the focus on supply chain security which has re-
sulted in a number of national and international initiatives.

Recent supply chain security initiatives have been (or are being) developed and implemented
by customs organisations because these are historically responsible for supervising the inter-
national flow of goods for compliance to import duty and health and safety regulations. This so
far has resulted in a number of different supply chain security requirements. Apart from re-
quirements to the management of supply chain security these customs driven regulations have
one common requirement. Customs want to have advanced information on the character of
cargo that is entering their jurisdiction in order to decide which cargo they will target with inten-
sified inspections, based on a risk assessment. The World Customs Organisation is attempting
to establish an umbrella which should harmonise these customs regulations on security man-
agement and advanced cargo information to facilitate international trade.

In response to the lack of a consistent set of standards for supply chain security the industry
has taken matters in its own hands. Whereas individual companies started to develop their own
systems, and so setting their own standard in the market, ISO has taken the initiative to start
developing a set of ISO documents which should fulfil the needs of industry and so establish a
better regulated and harmonised set of requirements to supply chain security.

A more detailed review of the current initiatives is given in Appendix C to this report.

4.4 Detailed supply chain security management requirements
In section 4.2 above the recommended mitigation measures which supply chain operators
need to implement to secure the supply chain are specified on a generic basis.

These requirements should in one way or another be incorporated in European Legislation, to
ensure that supply chain operators shall implement Security Management Systems
To that subject they are broken down into detailed prescriptive detailed minimum requirements, as given in figure 4.4.

### Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport Inland Waterway</th>
<th>Forwarding agents etc</th>
<th>Warehousing</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>General system requirements</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records (Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Human Resource Security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure that security critical staff including sub-contracted staff are screened and interviewed prior to employment and reasonable intervals.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Procedural security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement procedures how deviations and anomalies are handled</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organisation and within the supply chain are performed.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure inspection of confined spaces of the means of transport before (re)delivery</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forwarding agencies</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that a trusted employee is physically present during loading/unloading of the cargo unit to supervise the introduction or removal of cargo to prevent that the physical security of the cargo is inflicted. This supervision shall be uninterrupted from the start of the inspection until the cargo is sealed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that this trusted employee at closing of the cargo unit is providing it with a seal and record relevant details in compliance with the companies sealing procedure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure verification that seals on received cargo are intact and conform the appropriate records.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that empty or partially loaded cargo units are inspected to detect any security breach or compromising of the integrity of the unit immediately before loading</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all cargo is compliant with its documentation and manifests</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that any units partly packed at end of business are securely locked to restrict access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that origin site pre-alerts destination site before shipment. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that seals are stored under controlled conditions, not be used in numeric sequence and that records on seals are verified by a second person</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only containers, swap bodies, trailers etc are used which are acceptable to the regulatory authorities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check that all cargo entering the premises are properly sealed and that the seal or alternative access monitoring devices and where possible the cargo is compliant to its documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading and check pre-alert information from origin site. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that emptied cargo units are sealed again, with proper recording of such seals, or otherwise are secured against unauthorised access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only cargo is accepted to be loaded on the organisations means of conveyance which are properly marked, have the correct weight and documentation, and that the marking of the cargo (unit) and its seals are in accordance with the documentation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that cargo units, whether stuffed-up or empty, only will be loaded when they are properly sealed and this sealing is properly recorded.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that cargo is moved according to pre-defined schedules, including routes and stops, and unexpected delays and deviations are reported to the organisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements

**DESCRIPTION OF REQUIREMENT**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forwarding and transport</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that before loading, at departure and after each prolonged stop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>seals are checked for tampering, all readily accessible areas are</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>physical searched and internal/external compartments and panels and other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>potential places of concealment of illegal or illicit goods are</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>secured and/or inspected. These checks are to be recorded and records are</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to be kept for three months and be accessible to other actors in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>supply chain for verification.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure rerouting of dangerous cargo to avoid routine patterns</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that no unauthorised passengers are allowed on board.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that confined spaces are inspected after delivery or at</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>redelivery after maintenance or repair.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that vessels and barges are kept under constant surveillance,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>whether on route or boarded alongside and have adequate lightening to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>prevent intrusion.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that control rooms of traffic control centres are kept locked for</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>non-authorised persons.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that an analysis is made of the vulnerability of information systems,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the relevance to security of data and the implementation of adequate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>safeguards and firewalls.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that files and records are not removed from the office without</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>permission.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all computer users acknowledge receipt of, and consent to, the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT security policy as a condition of access to company systems.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all IT personnel with access to digital information, including</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>those with indirect access by means of administrative privilege, receive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>training on information security principles. For certain personnel, this</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>may include training on proper incident handling procedures.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that complete, legible and accurate documents, either electronically</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>or conventionally, are submitted timely to designated authorities, in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>format, means and at the time requested by them.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that security critical information is securely stored, only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accessible to authorised personnel and that the users of this information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>can be traced back.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the security officer regularly checks information access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>logs to identify any unusual or out-of-hours activity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that routines exist to securely cope with break downs and secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>back-up routines are followed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the transporter or cargo owner is informed when during the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processing of information it is noted that the progress or movement of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cargo deviates from pre-defined schedules.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that overages and shortages, as well as other anomalies, observed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>during the processing of information, are reported not only to the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>designated authorities, but also to the organisation(s) responsible for</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the processing of the cargo.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements

**DESCRIPTION OF REQUIREMENT**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forwarding agents</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that internal / external two way communication systems to contact</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure buildings containing critical working areas are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorised persons and goods.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, situated outside, are surrounded by perimeter fences which comply to the legal and statutory requirements</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas are fitted with doors, windows, gates and fences, provided with adequate locking devices.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, both inside and outside, as well as parking areas are provided with adequate lighting</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas are equipped with intrusion alarms or its equivalent and that alarms are subject to 24 hour response and real time monitoring</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that parking areas for private vehicles are well separated from critical working areas</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, where appropriate, are patrolled by guards, dogs and/or closed TV-circuits.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all loading and discharge valves and inspection hatches of dangerous cargo transports are provided with (pad)locks</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that dry-bulk cargo is covered by tarpaulins or hatches, which are properly sealed.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that international-, domestic-, high-value- and dangerous goods cargo is marked and segregated within the premises by a safe, caged or otherwise fenced-in area.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that dangerous goods are kept segregated from other cargo.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ensure that control cabins of means of conveyance, when not manned, are kept locked at all times and only employees of the organisation are allowed to have access.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that keys are kept under control of the driver/operator at all times.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that documentation containing cargo information is kept secure in these control cabins.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ensure that control cabins are equipped with an intrusion alarm.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that other internal or external compartments or panels are kept locked when not under surveillance.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that procedures are in place for reporting when unauthorised persons, un-manifested materials, or signs of tampering, are discovered.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ensure that no prolonged stops are made at isolated locations where normal social control can not be exercised, unless such location is equipped with adequate lightening (and fencing) according to the standards set by the designated authorities.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Water-way</th>
<th>Ware-housing</th>
<th>Forwarding agents etc</th>
<th>Shippers</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Controls</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only authorised staff has access to critical working areas. Controls shall include positive identification and recording of all arriving and leaving employees, suppliers, visitors, vendors and incoming vehicles and their drivers.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that visitors are not moving around the facilities without accompaniment of a trusted employee</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that unauthorised / unidentified persons are stopped and questioned</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that restricted areas are clearly marked as such and unauthorised access to these areas is prevented or raises an alarm.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that authorisation to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorised persons for which records shall be held.</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organisation for which records shall be held.</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Auditing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The organisation shall plan internal audits and follow-up possible improvements needed.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>The organisation shall be audited by an authorised external party to ensure compliance to above requirements</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Since the legislation should require that relevant operators implement a security management system these functional requirements shall include minimum requirements to the management system documentation and to continuous improvement as well.

There are two main options available to the European Commission for the formulation of such a set of security management requirements:

The European Commission can refer to the ISO PAS 28000 series (see also section 4.3: Current initiatives), which is presently under development and being matched with the results of this study and demand compliance from the operators to this international standard.
As an alternative the European Commission can incorporate detailed functional security requirements in its legislation based on the recommended mitigation measures in section 4.2 and the summary of the requirements in figure 4.4 above.

These detailed functional security requirements form the basis for parts of the cost benefit analyses in chapter 6 of this report and will provide adequate guidance to:

- Operators who shall implement security management in their organisations.
- Organisations which shall verify if such implementation is (still) adequate.

4.5 Accompanying instruments

In support of the implementation of the detailed security management requirements, as addressed in the previous section, two groups of instruments are identified.

1. Conditional instruments: These instruments aim to ensure the successful implementation of the security management requirements by creating the right conditions. Implementation of these instruments is mandatory for the implementation of the security management requirements. Three main conditional instruments have been identified:
   a. **Implementation**: To ensure proper implementation and maintenance of the security management requirements in the European supply chain.
   b. **Enforcement**: To ensuring continuous compliance to European security management system requirements by all participants in the supply chain.
c. Security awareness: To create the correct mindset in support of successful implementation of the security management requirements in the supply chain.

2. Supporting instruments: Most mitigation measures incorporated in the security management requirements (figure 4.4) are operator dependent. However, for a small number of measures European wide initiative in the form of an instrument/program is desirable, because the measures affect multiple operators simultaneously. Two of these instruments, which are considered to be supportive instruments, have been identified:

a. Employee vetting system: To prevent repetitive vetting for employees with high mobility (throughout Europe) and unstable short term work relationships.

b. Seal programme: To ensure a standardised seal program for all cargo passing through the supply chain from operator to operator between multiple countries.

In the next chapter required frameworks for the implementation of the security requirements and identified instruments are described.
5.0 Required frameworks

In this chapter the required frameworks for developing security management within EU supply chains (through the implementation EU supply chain security requirements) and for implementing the accompanying instruments, are developed and discussed.

5.1 Developing security management within EU supply chains

A summary of the detailed supply chain security requirements has been provided in figure 4.4 of section 4.4. These are the functional requirements to be implemented by the operators in order to secure their supply chains. As discussed in 4.4, this study recommends the development of EU legislation referring to the ISO PAS 28000 series which covers the functional security requirements instead of developing EU legislation which incorporates the security requirements. In this section the required framework for developing security management within EU supply chains are analysed based on the following topics.

1. Applicability
2. Responsibilities
3. Implementation approach
4. Relation to existing security schemes

5.1.1 Applicability of the supply chain security requirements

The supply chain, which for this study has been defined as stretching from the production site to the final distribution centre, combines in any order a number of process steps, where cargo is handled and/or transferred. Considering the interdependency of the steps, security of the entire supply chain can only be achieved through a combined and comprehensive effort. The supply chain is as weak as the weakest link and only if all steps in a supply chain operate secure, a supply chain can obtain a secure status.

The supply chain security requirements must therefore form a framework applicable to the whole supply chain and all its steps instead of a patchwork approach applicable to specific areas only. The focus on the complete supply chain does not exclude the possibility of more detailed approaches, standards or rules in specific areas as long as the minimum standards are upheld. In view of this, further development and evolution of security management content and approaches can focus on specific areas and does not need affect the whole supply chain.

Besides covering all supply chain process steps, the defined EU supply chain security requirements, are also applicable to operators in all four identified transport modes.

- Rail
- Road
- Inland shipping
- Short sea shipping

5.1.2 Security responsibilities: public/private partnership

Whereas supply chain management is industry’s responsibility, security is a state responsibility. Therefore, leaving the supply chain security to self regulation by industry would be irresponsible of any state. However, state responsibility for security does not mean that security
objectives cannot be achieved through common efforts in a collaborative state/industry approach. Where governments must set the regulatory framework, supervise and monitor the implementation of security in the supply chain, the practical implementation of security measures lies in the hands of the operators.

Operators in the supply chain can be companies such as:
- Manufacturers
- Cargo owners
- Importers
- Agents
- Transporters.
- Loading/Storage companies
- Maintenance companies
- Traffic controller
- Cargo information handlers

And their responsibilities include:
- Implementation and development of a security management system which includes the required security measures as defined in the EU security requirements.
- Further development of security management to a higher standard.
- Ensure resources are available for the implementation of the security management system and the security measures.

5.1.3 Implementation approach of security in the supply chain

From voluntary to mandatory
High levels of supply chain security combined with level playing fields for all operators can only be achieved through a mandatory security scheme where all operators must comply with the same EU security requirements. This will result in the same security levels in all supply chains, while no operators can obtain a competitive advantage by not complying to the requirements. However, there is general agreement that, in view of size and complexity of the markets and the required development supply chain security approaches must still undergo, that an immediate implementation of a mandatory system is not possible and can only be seen as a long term objective. A mandatory implementation by 2009 is recommended to coincide with the mandatory requirements from the revised Community Customs Code.

During the rolling out phase until compliance for all operators becomes mandatory, a voluntary approach is suggested. During this voluntary rolling out phase the operators are persuaded to participate and comply with the EU supply chain security requirements. Facilitations such as “green lanes” at security control inspections are to be applied as persuasion “carrots” and are further discussed in section 5.2.2.

The goal of the voluntary roll out leading up to the mandatory phase is to ensure a gradual implementation of supply chain security. This will allow for further maturing of security management thinking before it becomes mandatory. But more importantly it ensures a controlled and manageable implementation, which due to the sheer size and complexity of the markets is a necessity. Peak implementation, such as experienced during the ISPS implementation and known as the tsunami effect, is uncontrollable in supply chain security and needs to be avoided. Finally, gradual implementation will stimulate security awareness in all operators leading up to the mandatory phase.
During this study it has been assumed that 30% of the operators achieve compliance in 2007, the other 70% during 2008.

In the following sections the voluntary implementation approach will be further discussed.

Supply Chain Manager
To create sufficient momentum during the voluntary phase, before straight compliance is demanded in 2009, a supply chain manager approach should introduce security management into the EU supply chains.

One operator, generally the cargo owner responsible for transportation of the goods, is responsible for the supply chain, the selection of all its operators and its security. In order to create a secure supply chain, this operator, known as the ‘Supply Chain Manager’ selects only certified secure operators (according to the requirements defined in this study) to be part of his supply chain. While individual operators are responsible for implementing the security measures in their organisations, the Supply Chain Manager will guarantee that he utilises only secure operators, hence ensuring a secure supply chain.

During the voluntary phase Member States should motivate the Supply Chain Managers to set up secure supply chains. This will lead to “forced” gradual implementation of security management into the market, because each Supply Chain Manager’s voluntary decision to make his supply chain secure, makes for all participating operators the compliance to the security requirements and implementation of a security management system mandatory. This voluntary implementation can be compared to a champagne pyramid being filled from the top. The top glass is the Supply Chain Manager. When he is persuaded to become a secure operator and create secure supply chains, he will demand his suppliers and subcontrac-

**ISPS Code** *(ref: Appendix C)*

_The International Shipping and Port facilities Security code is international security regulation applicable for ships and port facilities, which contain mandatory requirements to be met by operators through the implementation of defined preventive measures._

_The mandatory date was not preceded by a voluntary phase, which resulted in a massive peak implementation shortly before the mandatory date, known as the tsunami effect._
tors, represented by the second row of glasses, to be secure operators. However in order for these sub-contractors and suppliers to be secure operators, their suppliers and operators (the next row) are also required to become secure operators. Security management trickles down into the supply chain like the champagne flows down the pyramid. To eventually achieve a complete secure supply chain, the Supply Chain Manager needs to have a transparent supply chain pyramid in which all levels have implemented the required security measures.

Based on the above approach, when moving down the pyramid, security becomes a mandatory requirement in order for the operator to stay in business. However, in reverse order, being able to be part of new supply chains or be preferred operator for a client is an incentive for operators to implement security.

Successful implementation of this approach is dependent on the creation of transparency in the supply chain, where the Supply Chain Managers know who are involved in the supply chain and ensures that all involved are certified secure operators.

The application of a ‘Supply Chain Manager’ approach also has impact on the viable options for audit programs which will be discussed in more detail in section 5.2.1.

**C-TPAT (ref: Appendix C)**

*The US Customs-Trade Partnership Against Terrorism program is a voluntary partnership between US Customs and the import trade community to reduce threat risk and to certify companies that have secure supply chains. The objective is to strengthen and fortify supply chains importing into the US against terrorism and to balance needs for increased security measures in conjunction with a reduction in unnecessary delays due to customs interventions.*

*Similar to the proposed Supply Chain Manager concept, the C-TPAT program requires the importer to ensure the integrity of their security practices and to communicate security guidelines to their business partners at each part of that supply chain. The program addresses physical security, personnel security and service provider requirements.*

*Is however criticised heavily because of lack of verification (audits) which makes the whole programme very much a paper exercise.*
Identification of Supply Chain Managers
Supply Chain Managers can be identified in two formats:

- Sellers of cargo which are responsible for transport of the cargo to the destination. E.g. manufacturers and distributors.
- Buyers of cargo which are responsible for transport of the cargo from buying point to destination. E.g. importers.

In general Supply Chain Managers can be identified as the owner of the cargo responsible for its transport. Implicitly this means that each time the ownership of the cargo changes the Supply Chain Manager changes. If a non-secure Supply Chain Manager is followed by a secure Supply Chain Manager then the secure Supply Chain Manager is responsible for inspecting the cargo to re-secure the supply chain.

To be able to identify whether a secure operator is also part of secure supply chain, the freight documents accompanying the goods must also include who is Supply Chain Manager and thus responsible for the security of the cargo.

Advantages of supply chain manager approach

- Supply chains are characterised by large numbers of enterprises. This makes centralised control and supervision by the national governments over implementation of security in the supply chains very labour intensive. Identifying Supply Chain Managers each responsible for their own supply chain allows a government focus on these Supply Chain Managers and their control over their supply chain instead of having to focus on all operators.
- ‘Authorised Economic Operator’ and ‘Known Consigner’ are concepts applied respectively the Community Customs rules and the Community’s airport security regulations. The same concept of a ‘secure operator’ lends itself to the field of supply chain security, where proved compliance with the baseline security requirements would result in facilitations and reduced security controls. However, these so called “green lane” facilitations can only be applied if all links in the supply chain are secure, which requires all operators from production to final delivery to be secure operators. The supply chain manager approach contributes to transparency of the whole supply chain and guarantees security of the whole supply chain.
- The supply chain manager approach can be seen as an implementation catalyst through its pyramid implementation as discussed above. Persuasion of one supply chain manager to participate, results in security management being implemented in all operators involved in his respective supply chains. This will created a “forced” gradual implementation instead of a peak implementation, as seen with ISPS, and expected if the decision to implement is left to all individual operators.

Multinationals such as Philips and Siemens already actively apply the Supply Chain Manager approach with respect to the protection of the supply chain against theft, but also brand protection.

Both multinationals can be identified as supply chain managers which take responsibility for all their supply chains of internal transports of half products between their own factories but also transports of the end products until the first buyer. For each of these supply chains Siemens and Philips carefully select all participating operators which can best guarantee the protection of their goods.

Similar approaches have been taken in the food sector. Where new regulations demand transparency of the whole supply chain from animal to consumer.
Top 100 focus
In this voluntary approach where the ‘Supply Chain Managers’ are end responsible for security in their supply chains, the National Governments will need to persuade the ‘Supply Chain Managers’ to implement security management in their supply chains and fulfil the EU security requirements. This study recommends an initial focus on the industrial leaders, such as the TOP 100 manufacturers and importers to initiate the implementation of security management. Because of the pyramid format of their supply chains, it is expected that if the TOP 100 implement security management in their supply chains, a large portion of the supply chain operators will be covered.

There will be operators, which will be part of supply chains whose ‘Supply Chain Managers’ have not been persuaded to implement supply chain security, or which operate on lower echelons of the transport market and fall outside of major supply chain “pyramids”. These operators are independently free to implement security management in their organisations. For the operators which are not covered a special awareness program needs to be run to inform them of the deadline when the security requirements become compulsory.

Benefits to stimulate implementation
In chapter 6 the possible benefits of implementing security management in the supply chain are defined and discussed. These benefits may stimulate the ‘Supply Chain Managers’ and the operators in implementing security management in the supply chain to obtain:

• Sustainability and resilience of organisations.
• Trade facilitation.
• Reduction of cargo theft.
• Prevention of damage to brand and reputation.
• Increased efficiency and transparency.

Evolution of the security management concepts
During the voluntary roll out period security management will evolve on its content and approach. Security management is relatively new and based on initial implementations and experiences it will undergo further refinement. Implementation of security management is proposed for the whole supply chain, however different maturity levels will exist. This requires a joint cooperation between operators and national governments.

Furthermore, experience will be gained by custom authorities as well which needs to be incorporated to ensure continued connectivity.

The mandatory phase
As of 2009, coinciding with the EU customs code, implementation of security management in the supply chains will become mandatory. All operators in the supply chain must from that
moment comply with the drafted supply chain security requirements to ensure high levels of security in all supply chains combined with level playing fields for all operators.

The role of the Supply Chain Manager in securing the supply chain will diminish once supply chain security enters the mandatory phase. Since all operators must comply with the requirements the security of the supply chain will automatically be ensured. The supply chain manager approach therefore remains mainly a catalyst to implementation during the voluntary phase.

5.1.4 Relation to existing security schemes

At present there are a number of transport security schemes already in force in the EU. These existing security schemes can be found in the maritime and air transport sector, as previously discussed in this chapter. Besides the EU customs sector is developing its own requirements to exporters and importers. The goal of the supply chain security scheme is not to replace but to complement these security schemes so creating a comprehensive and integrated security approach which covers all transport sectors, including air and maritime and which integrates with global supply chain security.

The presence of the existing security schemes can have two positive impacts on the implementation of the supply chain security scheme.

1. Operators already participating in the Community Customs code as Authorised Economic Operator require no investment to fulfil the supply chain security requirements. The barrier to the supply chain requirements is further reduced when the EU legislation, the ISO PAS 28000 series and the Community Customs code contain similar supply chain security requirements.

2. Considering that the EU legislation complements the other security schemes, “green lanes” can be created crossing through the various schemes. These integrated “green lanes” will motivate operators to be part of all security schemes to create maximum benefit for themselves.

The different security schemes should aim for mutual recognition. Security conditions should be made compatible and Secure Operators must be recognised as Secure Operators, Authorised Economic Operators or Known Consignors and vice versa. Fulfilment of one security scheme results in recognition in the other schemes. The combination of all schemes in one standard such as the ISO PAS 28000 series will be a step towards compatibility of the security schemes.

5.2 Ensure successful implementation

One of the two types of accompanying instruments identified in section 4.5 are the conditional instruments. These mandatory instruments ensure successful implementation of the security management requirements. Three instruments have been identified:

- Implementation through audit
- Enforcement through inspection
- Security awareness
For each instrument the required frameworks will be discussed below.

5.2.1 Implementation through audit
Implementing legislation which contains security requirements to which supply chain operators should comply, creates a need for audit schemes for:

1. Ensuring the implementation and maintenance of the security management systems and mitigation measures.

2. Creation of a secure operator label by which supply chains and operators who have successfully implemented the minimum requirements can be recognised.

Four different audit approaches can be taken each with advantages and disadvantages. The key (dis)advantage, however, is the degree of confidence the approach provides to the Member States that the security measures have been implemented correctly, where, as always, a balance needs to be sought between confidence and costs.

a) **Self assessment by industry (1st party):** Each operator performs self assessments to guide and determine the states of implementation of the mitigation measures and his security management system and confirms this with the designated authorities.

b) **2nd party assessment by industry:** Second parties in the industry such as industrial leaders not only assess the status and degree of implementation of security management in their own organisation but also in their subcontractors’ organisations.

c) **3rd party certification:** Each operator’s implementation of security management is assessed by an independent third party who has been authorised as a Recognised Security Organisation by a Member State or has gone through a notification process by the national accreditation bodies. Successful implementation of the measures and security management system results in official certification of the operator by the RSO or the accredited certification body as Secure Operator.

d) **Governmental inspections:** Newly to establish or existing government inspectorates assess the operators’ implementation of the security management requirements. Successful implementation of the measures and security management results in official recognition as Secure Operator.

C-TPAT (ref. Appendix C)

The C-TPAT scheme, as implemented by the US (ref. report 2, section 4.2.) is largely relying on:
- 1st party certification (self declaration) or
- 2nd party certification where the importers into the US shall ensure that the C-TPAT requirements are properly implemented throughout his supply chain.

Based on proper submittal of documents US customs offer reduced cargo inspections at US and foreign ports. The US Government Accountability Office (the US equivalent to the European Court of Auditors) however has recently heavily criticised the program since the lack of verification of the effective implementation of companies’ security programs does not justify reduced inspections and hence creates a security laps at the outside borders of the US.
Although self assessment and 2nd party assessment are cost-neutral approaches to the Member States, the degree of confidence and the consistency they provide are low. They are therefore not recommended by this study, with 3rd party certification and governmental inspections remaining as the two viable approaches. Their advantages and disadvantages are presented in figure 5.2.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provides high confidence to the Member States.</td>
<td>• Company oriented → not the chain but each single operator in the chain gets certified.</td>
</tr>
<tr>
<td>• Regulatory and commercially driven → based on regulation and commercial requirements on being certified.</td>
<td>• Acceptance time by industry → time to accept and accommodate.</td>
</tr>
<tr>
<td>• Transparency → clear criteria and certification method which is equal to all.</td>
<td>• Availability of resources → both quantity and quality resources need to be developed by certification bodies.</td>
</tr>
<tr>
<td>• Level playing field for all operators → high consistency throughout the EU via the International Certification Accreditation Board (ICAB).</td>
<td>• Expenses for the industry → industry pay for the certification, cost neutral to the Member States.</td>
</tr>
<tr>
<td>• Low price to trade → single audits per operator.</td>
<td>• Deadline can be defined → by the authorities.</td>
</tr>
<tr>
<td>• High credibility → independence of notified bodies.</td>
<td>• Governmental control → through notification of certification bodies.</td>
</tr>
<tr>
<td>• Governmental control → through notification of certification bodies.</td>
<td>• Full governmental control → government performs the audits.</td>
</tr>
<tr>
<td>• Deadline can be defined → by the authorities.</td>
<td>• High expenses for the government → government pay for the audits.</td>
</tr>
</tbody>
</table>

Figure 5.2: Advantages and disadvantages of 3rd party certification and governmental inspections

Auditing the Supply Chain Manager

It is recommended that Member States take the responsibility to implement adequate audit schemes under their jurisdiction which provide a high enough level of confidence. Either they should establish their own inspectorates to verify adequate implementation of security management systems, which will substitute a large burden for their budget.

Alternatively they can delegate this to Recognised Security Organisations or they agree with their national accreditation body that these develop the criteria and rules of the game which allow management system certification bodies to become authorised to submit 3rd party certificates of compliance to the EU supply chain security requirements.

ISPS Code (ref. Appendix C)

For the certification of vessels to the ISPS Code most flag states have delegated this task to the more reputable classification societies, who they nominated as their RSO. The criteria on which such delegations were based were not always consistent and well defined.

Increasingly Member States have delegated some of their inspectorate tasks to independent 3rd party certification bodies, provided they are approved by their national accreditation body and they fulfil a number of additional requirements which are defined by the responsible department and verified either by this department or by the accreditation body, when they are considered to be competent in the pertaining subject. An example is product certification against the EU Pressurised Equipment Directive.
Auditing the operators
Because the ‘Supply Chain Manager’ is designated as responsible for the security of his supply chain, one could argue a 2nd party assessment approach. However, this approach, where the ‘Supply Chain Manager’ verifies adequate implementation has already been deemed undesirable and besides:

- It will result in repetitive audits since most operators are part of multiple supply chains and are therefore under the scrutiny of multiple ‘Supply Chain Managers’.
- International competition will be disrupted due to difference in interpretation between the different ‘Supply Chain Managers’. Equal criteria and consistent interpretation will be difficult to control.
- No formal secure label can be issued to operators, because ‘Supply Chain Managers’ are no formal audit and inspection bodies.

Auditing of the operators must therefore also be approached through either 3rd party certification or governmental inspections.

Level playing fields
Irrespective whether Member States opt for own inspectorates or 3rd party involvement for the auditing of the ‘Supply Chain Managers’ and Supply Chain Operators, it is essential that the Commission takes its responsibility to ensure that international competition is not disrupted and that an un-equal level of security throughout the Union is created by different interpretation or execution by the different Member States.

When Member States opt for the use of accreditation bodies and 3rd party certification bodies, the accreditation bodies will define the criteria and rules of the game. The Commission will need to define audit criteria and rules in line with the accreditation practices for the Member States wishing to opt for own inspectorates or Recognised Security Organisations. These are the minimum criteria to which verification organisations and its staff shall comply and also shall be charged with the authority to investigate and correct when complaints are raised about companies or organisations which disrupt the level playing field within the Union.

Secure operator label
Successfully audited operators should receive a secure operator label to make them recognisable as operators who are compliant to the EU supply chain security requirements and thus may enjoy the benefits which comes with this status. Mutual recognition between the national audit schemes need to be assured to ensure that secure operator labels are valid and recognised in all Member States.

In order to maintain the level of confidence that operators maintain proper implementation of the requirements, periodic re-audits are necessary.

Advantages of EU secure operator label
- Security control measures can be focused on operators not part of secure supply chains.
- A mutual recognised security label will support a common security approach which will contribute to predictability for both the operator and the Member States. The operator will benefit from uniform recognition and the Member States will know all operators are audited to the same security level and criteria.
- Interconnectivity can be setup with the Known Consignor and the Authorised Economic Operator concepts in the aviation and customs sectors.
• Business recognition as operators can demonstrate their security compliance to partners and clients.

5.2.2 Enforcement through inspection

While an audit scheme, as considered in the previous section, ensures that operators implement and maintain their security management systems, this does not guarantee operators’ eligibility to implement EU’s supply chain security requirements will (continuous) comply with these requirements and the developed security management systems. An enforcement/policing regime is therefore required as a conditional instrument, which is based on an inspection scheme and complemented with stick and carrot arrangements. During the voluntary phase the enforcement program will mainly rely on the carrot arrangements, while stick arrangements will contribute during the mandatory phase.

5.2.2.1 Inspection scheme

Security control vs. security management compliance inspections

Two types of inspections can be identified:

1. **Security control inspections:** are aimed at operators and their cargo to screen on possible security threats. Goal is to increase the general security level.

2. **Security management compliance inspections:** are aimed at operators with a secure operator status to verify compliance to the security measures.

The enforcement program is centred around the security management compliance inspections with the goal to enforce continuous compliance to the security management system and the EU supply chain security requirements.

Two tiered inspection approach

The study recommends a two tiered inspection approach based on routine and targeted inspections:

1. **Routine inspections:** routine inspections are performed in all aspects of the supply chain such as the cargo, means of transport, critical working areas and the operators’ organisations to determine general compliance.

2. **Targeted inspections based on intelligence:** targeted inspections are performed in case suspected non compliance by an operator or during heightened terrorist threats in specific areas of the supply chain.

Supply chain inspection

During an inspection the inspector should not only verify compliance of the inspected company but also identify the origin and destination of the cargo to determine the traceability of the cargo and the security of the supply chain. In order for the supply chain to be secure, the origin and destination of the cargo need to be identified as certified secure operators. Verification of the security of the origin and destination can take place in previous and subsequent inspections of which the results are catalogued in the database.
Alternative site inspection

As described above, inspections are not focused on one point in the supply chain. For each point in the supply the security of the origin and destination of the cargo needs to be verified as a certified secure operator. Inspections therefore move up and down the supply chain verifying both the nodes and the links.

- **Nodes**: These are fixed positions in the supply chain such as storage facilities, loading facilities, maintenance workshops, producing facilities, distribution facilities, etc.

- **Links**: These are mobile positions in the supply chain such as the means of transport and the cargo travelling from one node to another.

Authorities to perform inspections

The study proposes the combination of the inspection activities with existing authorities

- **Customs**: When cargo enters the European Union security compliance inspections can be combined with customs inspections at the border.

- **Authorities enforcing compliance to transport safety regulations**: At present in most EU Member States authorities are already in place to enforce compliance to transport safety regulations. The activities of these authorities can be broadened to include security control inspections and verification of compliance for certified secure operators. An inventory of existing authorities in various Member States, concluded that Member States had specific inspectorates in place for road traffic inspections, while other bodies covered the railway and shipping.

- **Authorities involving labour and safety inspections**: Since the supply chain includes large numbers of manufacturers and forwarders or other organisations to facilitate the logistic process, it is recommended that Member States involve labour-safety inspectorates in this policing task to cover security inspections in nodes.

Database of certified secure companies

All certified secure companies need to be incorporated in a database. This allows security inspections to be incorporated with regular safety inspections. The inspector can check if the company is certified secure and accordingly verify compliance. Inspection results can be uploaded into the database.
5.2.2.2 Carrot and stick arrangements

Enforcement regimes require repercussions in order to be effective. Without repercussions verifications would remain to be observations and a non-compliance would not result in corrective actions. Repercussions can be shaped as either the proverbial carrot or the stick. The stimulant versus the pressure.

The carrot: "green lane" treatment

Carrots are most effective during the voluntary phase when they need to stimulate operators to implement security management in their organisations. An effective stimulant would be the development of "green lanes" for certified secure operators.

Authorities responsible for security and security inspections give preferential treatment and benefits to the certified secure operators. They allow them to benefit from facilitations and simplifications of security control measures during inspections. While non secure operators must face a complete inspection, secure operators can pass with a simple verification of the cargo documents to see whether it is a secure operator/supply chain. "Green lane" treatment should interconnect with secure maritime, air transport and export through customs, creating a preferential treatment lane throughout the international supply chain crossing various transport modes. Accordingly the focus of the inspections can be on the operators not partaking in the security schemes, however not forfeiting the right to inspect secure operators when warranted or to spot check compliance.

Operators which have implemented security management systems and have received a secure operator label but which were inspected to be non compliant, lose their secure operator status and their access to the "green lanes". Serious breaches should result in a status withdrawal for longer periods of time, e.g. minimum 1 to 2 years.

Note that “green lane” treatment does not result in complete forfeit for all inspections. Operators will continue to be subjected to incidental inspections to spot check compliance.

The stick: financial penalties

Sticks only can be applied during the mandatory phase, where operators which are found to be non compliant are punished and thus pressured to solve their non-conformities. Recommended sticks during the mandatory phase are financial penalties.

In a financial penalty approach operators which have received a secure operator label and are found to be non-compliant at inspections are financially penalised for the non-conformity with a fine by the Member States' inspectorates.

---

Dangerous goods (ADR) (ref. Appendix C)

In the general provisions of the ADR checks and other support measures are defined to ensure compliance with the safety requirements for the transport of dangerous goods by road. The provision states that the responsible transport/safety authorities in each participating country may, on their national territory, at any time conduct spot checks to verify whether the requirements concerning the carriage of dangerous goods have been met. The participants shall, without delay, in the context of these obligations provide the authorities and their agents with access and the necessary information for carrying out the check. In the case of non-conformities, appropriate measures are prescribed or the transport is immobilised.
### Air safety regulations

Compliance to civil air regulations by international carriers is verified by national inspectorates, by means of spot check at airports on their national territory. High risk carriers and carriers with previous non-conformities are subjected to increased scrutiny by the inspectorates. In case major non-conformities are observed the inspectorates have the authority to deny carriers landing rights to the national airports as a stick to force compliance.

---

5.2.2.3 Relationship inspections and repercussions

A direct relationship exists between the type of repercussion and the amount of inspections required to be performed.

During the voluntary roll out phase an immediate dramatic increase of the number of security control inspections is required in order for the “green lane” treatment to become an effective stimulant. The present amount of security control inspections in the supply chain and disturbance to the operators are of such a low level, that “green lane” simplifications will have nil impact to the operators. Only by increasing the security control inspections to such a level that they seriously impact the operations, will the “green lane” be seen as beneficiary. After security management becomes mandatory all operators will need to comply and “green lane” treatment can no longer be applied. The number of security control inspections can also be reduced to spot check levels.

![Figure 5.4: required inspection capacity](image)

The number of participating operators will gradually increase during the voluntary phase, resulting in a gradual increase of compliance inspections to monitor these operators. When the supply chain security scheme becomes mandatory and fines are introduced to pressure compliance the compliance inspections will see a sharp increase to cope with the sharp increase of operators participating. However, the number of compliance inspections during the mandatory will only be a fraction of the number of required security control inspections during the voluntary phase. The relationship between the number of inspections and the repercussion schemes is presented in the graph below.

Given the fact that, once mandatory, 2,5 million enterprises in the Union are effected by the requirement to implement security Management in their organisation. The present level of (safety related) traffic inspections seems to be insufficient to achieve the objective of security
related routine inspections. It is therefore recommended to permanently double the present amount of routine traffic inspections in the Member States when the program enters the mandatory phase. The peak in the above graph can be considered temporary. The cost calculations for inspections, to be found in chapter 6, will be based on the mandatory situation when the inspections have been doubled.

5.2.3 Increasing awareness
Security awareness has already in section 4.2 been identified as a measure to identify suspicious behaviour related to blackmail of staff or infiltration in the organisation. However, security awareness programs can also be observed from a generic context. Similar to other management systems, security management is related to human behaviour. There is a deep interaction between human behaviour and security management. On the one hand security management aims to influence human behaviour into more secure patterns. On the other hand the success of security management is fully dependent on human behaviour and a security mind set of people. In order to be able to influence people into security best practice behaviours, they need to be security aware.

The implementation of security awareness programs throughout the EU Member States is therefore recommended as a conditional instrument to influence the mind set of all workers in the supply chain and to contribute to the successful implementation of the mitigation measures and security management in the supply chain.

Awareness on the work floor
The security measures specified in chapter 4 are to be implemented on operational level of the supply chain. To support successful implementation of security management in the supply chain awareness must be created on the same organisational level as where the measures are being implemented.

Awareness programs must, therefore, be aimed at, but more importantly be organised on, the work floor of the supply chain by the operators and the industry. The Member States must, through the use of trade and industry associations, support the industry and operators in implementing the security awareness programs to raise the over all security awareness and mind set. Possible examples of support are the supply of awareness posters, films and advertisements.

Realising that keeping up the awareness about the relevance of national awareness programmes the Commission shall continuously stimulate the Member States on this issue, develop where relevant awareness tools which are visibly similar throughout the international supply chains of Europe and support Member States in their efforts through the use of international trade- and industry associations.

Two way information
Active participation stimulates awareness. Awareness therefore concerns not only providing information to employees to inform them about security and terrorism, but also providing communication channels through which they can convey their suspicions. Communication channels allows the employees to act upon any suspicious behaviour giving purpose to being aware.
5.3 Supporting implementation

While the minimum measures defined in figure 4.4, shall be further developed and implemented by the operator, for a few of those measures European wide initiatives in the form of an instrument / program are helpful. Two of these instruments, which are considered to be supportive instruments to the implementation of security management in the supply chain, have been identified:

- Employee vetting system
- Seal programme

For each instrument the required frameworks will be discussed below.

5.3.1 Employee vetting system

In chapter 4 employee vetting was defined as a mitigation measure to deny unauthorised access to the organisation. It entails the performing of security background checks on employees to prevent infiltration by terrorists. The measure is included in the EU security requirements and the operational responsibility for implementation lies with the supply chain operators. However, to support the operators and relief the vetting burden of specifically high mobile employees an European vetting system is proposed.

European vetting programme

As discussed in chapter 4 three types of employee categories exist indicated by low, medium and high mobility (see also 2.3.3 ad. 3). Employees with high mobility are those who have short term and unstable work relationships and seek employment throughout Europe. These employees may be working for multiple employers during a span of just one year. For operators employing a high number of these high mobility employees, vetting is a heavy burden on the organisation, due continuous influx of new employees. Furthermore the employees are vetted multiple times as they move from one organisation to another. A European vetting programme is therefore recommended specifically for employees with high mobility to prevent multiple vetting of these employees. Responsibility for the vetting of employees with stable work relations can remain with their employers.

In such a centralised programme the employees with high mobility are vetted once in trusted organisations and their vetting results are stored in a central database. Employers either have access to the database or receive proof of successful vetting. The vetting is valid in the whole EU and is sufficient to comply with the vetting requirements.
Whether such a system is developed and managed by the Member States, by national organisations which are coordinated on national or European level or by the private sector, under close supervision of the authorities to ensure compliance with tight integrity requirements is a decision which needs to be taken.

There are four main aspects to consider:

- **Vetting criteria**: the criteria on which an employee is being vetted and the required information sources. As source previous employers, criminal records and for dangerous goods intelligence service information should be used.
- **Vetting method**: methods available to perform the actual vetting, which can range from 3rd party personnel certification to vetting by authorities to approved employment agencies.
- **Storage of vetting results**: vetting results need to be stored in central databases, accessible for future updates.
- **Proof of vetting**: vetted personnel need to be able to provide proof of vetting to their employers.

**Privacy restrictions**

Vetting of staff and storage of data is a sensitive area which easily conflicts with privacy legislation. Each Member State has its own privacy legislation and is free to accept or reject an EU vetting programme. Based on a survey in the 25 EU Member States it was determined that national privacy legislation is both similar and strict on the application of databases which incorporate personal information. Personal data, such as the data which is obtained from a background screening may only be incorporated in a vetting database with explicit consent from the employee.

This entails that employees who give consent to being included in the programme will only undergo one vetting, while employees who do not give consent continue to undergo vetting each time they change from employer.

**Vetting requirements**

Each Member State together with their trade/industry and labour associations must agree upon whether or not to set up a vetting programme and how a vetting database can best be developed and maintained. The recommended solution is to utilise certified Secure Operators and specialised labour agencies to perform the vetting and maintain the database.

Since each Member State is responsible for their own vetting programme it is recommended that the European Commission defines the minimum criteria and procedures for vetting and verifies their application throughout the Member States participating in the program. This will ensure that vetting results are valid in all Member States while maintaining equal level of security and level playing fields among the Member States.
5.3.2 Seal programme
The mitigation measures as defined chapter 4 include the application of seals on cargo containments. Seals make it possible for forwarders, law enforcement officers and for the recipient of shipments to easily verify if cargo has been accessed, based on whether or not the seals have been tampered with.

The fundamental responsibility for the safe and secure loading and sealing of cargo containments rests with the (re)stuffer or the shipper. Consequently each operator in possession of the cargo has security responsibilities while cargo is entrusted to them, whether at rest at a node or while moving between nodes. Those responsibilities include:

- Protecting the physical goods from tampering, theft, and damage.
- Protecting the information related to the goods from tampering and unauthorised access. This responsibility applies equally to times before, during and after having custody of the goods.

EU seal framework
The operators are, where applicable, responsible for setting up their seal program. They shall ensure that unused seals are securely stored, that used seals are correctly affixed and recorded, that containments, opened for inspections, are correctly resealed etc.

Even though the operators are fundamentally responsible, the development of a standard for seal integrity program as a supportive instrument is both desirable and recommended because the cargo is passed from operator to operator from country to country. Therefore, there will exist no ambiguity on what a seal is. The Commission must provide standardisation on seals and provide a framework within which the different operators can develop their seal programs and procedures.

A standard for seal integrity program must focus on two aspects. First of all, it must describe the technical requirements and aspects of the seals, defining the mechanical seal strength, marking and operation of seals. Only approved seals are to be used by the operators. For this the EU can:

- Develop their own seal requirements in the form of new legislation.
- Refer to ISO PAS 17712, which defines mechanical seals, and demand compliance from the operators. The WCO seal program makes a similar reference to this ISO PAS.

The second aspect of the EU seal integrity program must describe the procedural requirements which the operators must meet when implementing their seal program. Here also the EU can either develop new EU requirements or refer to an existing program such as the one from WCO. The procedures must include, amongst others, the following items:

- Application of seals
  - During loading
  - Intermediate terminal/warehouse
- Inspection of seals
  - By receiving party
  - At reloading
  - At unloading
  - Check with accompanying documentation
- Changing of seals
  - Inspections by law enforcement agencies
• What to do in case of tampering
  o Inform sending party
  o Note discrepancy in documentation
  o Alert law enforcement
  o If no notification requirement exists, refuse custody

**WCO Seal Program**

The WCO seal program defines the responsibilities of the involved operators at different steps in the supply chain which includes:

- Crossing cutting responsibilities which apply to all operators at all steps.
- Stuffing site responsibilities
- Intermediate terminal and warehouses responsibilities; and
- Unloading site responsibilities

At each step the program identifies who is responsible for affixing and removing the seal, documenting the seal, verifying the seal and what to do in case of a tampered seal.
6.0 Cost and benefits of protecting the supply chain

Basis for this chapter is an analysis of the cost and benefits connected to the instruments which the European Union are recommended to implement to improve the security of the supply chains as defined in chapter 4 and 5 of this report.

An assessment has been made of the financial impact which the implementation of security management in the regular supply chains within the EU 25 will have.

The assessment of the cost has been based upon data derived from EUROSTAT and estimates of the cost on the specific measures as defined in figure 4.4 above. Mainly EUROSTAT data were used from 2001 and 2002 since more recent data sets were not complete or refined enough.

The benefits which implementation of security management throughout the supply chain creates for industry have been assessed, partly on a qualitative and partly on a quantitative basis. Quantitative data has been derived from knowledge in public domain and specific publications.

6.1 Cost to industry for implementing security management

6.1.1 Number of enterprises involved

To make a proper assessment, cargo transport related datasets were utilised from NACE Group I “Transportation”. The following categories are separately considered:

- Road transportation of cargo.
- Rail Transportation of cargo.
- Transportation by inland waterways.
- Storage, warehousing and cargo terminals.
- Other logistic support, like forwarders, agents and other mediators.

Since further it can be assumed that potentially all manufacturers and construction companies are part of supply chains data from NACE group D (Manufacturing) and F (Construction) were consulted as well.

In each sector, EUROSTAT identifies four different company sizes in their datasets: Micro (< 10 employees), small (< 50 employees), medium (< 250 employees) and large (> 250 employees)

The basis for the assessment of cost to industry has been the total number of enterprises in the EU25, split-up by size and sector. These are given in Figure 6.1
Number of enterprises in EU 25, potentially affected by supply chain security requirements.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail repair/maintenance shops</td>
<td>1.500</td>
<td>1.000</td>
<td>2.500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Road transport</td>
<td>450.000</td>
<td>50.000</td>
<td>3.000</td>
<td>300</td>
<td>503.300</td>
</tr>
<tr>
<td>Rail transport</td>
<td>8</td>
<td>35</td>
<td>43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inland shipping</td>
<td>8.300</td>
<td>300</td>
<td>8.600</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warehousing</td>
<td>3.000</td>
<td>24.000</td>
<td>28.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other logistic support</td>
<td>54.000</td>
<td>5.000</td>
<td>60.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total logistic sector</strong></td>
<td><strong>515.300</strong></td>
<td><strong>80.800</strong></td>
<td><strong>6.008</strong></td>
<td><strong>335</strong></td>
<td><strong>602.443</strong></td>
</tr>
<tr>
<td>Manufacturers NACE Group D</td>
<td>1.443.000</td>
<td>282.000</td>
<td>72.000</td>
<td>17.000</td>
<td>1.814.000</td>
</tr>
<tr>
<td>Construction NACE Group E</td>
<td>2.250.000</td>
<td>62.000</td>
<td>20.000</td>
<td>2.000</td>
<td>2.334.000</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>4.208.300</strong></td>
<td><strong>424.800</strong></td>
<td><strong>98.008</strong></td>
<td><strong>19.335</strong></td>
<td><strong>4.750.443</strong></td>
</tr>
</tbody>
</table>

Figure 6.1: Total number of enterprises considered

There are approximately 4.75 million enterprises in the EU25 affected by the supply chain security requirements. However it would not be realistic to include all these enterprises in the assessment of the total cost to industry.

In particular larger companies will operate on export markets where they (are going to) meet security requirements, imposed on them by customs on a voluntary basis. The response to the US C-TPAT scheme shows that custom regimes have a strong appeal to exporters since compliance to customs security requirements drastically reduces the time consuming inspection procedures at the point of import/export. Since this report advocates (and assumes) a synchronisation of the requirements between the proposed supply chain legislation and the custom requirements, those companies which are (going to be) in compliance with custom requirements also (are going to) meet the supply chain security requirements. One of the objectives of the new supply chain legislation is the avoidance of duplication of requirements and the achievement of mutual recognition to create one standard.

Therefore, an estimation has been made of the percentage of companies that will comply with these custom requirements, which includes manufacturers of high value high tech goods which comply already with the TAPA requirements, and hence reap the benefits that customs (will) provide. While these companies remain to be affected by the supply chain requirements, they will be excluded from the total cost calculation since have already made the costs and reap the benefits.

Besides it is estimated that especially micro enterprises in the manufacturing sector (partly) and the construction sector (100%) are local operators which are not participating in any supply chain. These include local small (often self employed) contractors such as bricklayers and carpenters which only serve local construction markets and local manufacturers such as small production shops which only produce on demand for the local market. These companies do not export their products outside the region and transport the goods themselves. However in the proposed mandatory phase it will be difficult to make a distinction whether or not a company is excluded from the supply chain and thus from the security requirements. In addition, participation in supply chains is variable. Therefore, the above argument cannot serve as a rule for exclusion. All micro companies must comply with the requirements.
The estimated percentage and number of enterprises which are not included in the assessment is given in figure 6.2

**Number of enterprises in the EU 25 which will comply with EU and/or US customs and TAPA requirements**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail repair/maintenance shops</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Road transport</td>
<td>5</td>
<td>2,500</td>
<td>25</td>
<td>75</td>
</tr>
<tr>
<td>Rail transport</td>
<td></td>
<td></td>
<td>25</td>
<td>2</td>
</tr>
<tr>
<td>Inland shipping</td>
<td>10</td>
<td>830</td>
<td>50</td>
<td>150</td>
</tr>
<tr>
<td>Warehousing</td>
<td>5</td>
<td>150</td>
<td>10</td>
<td>2,400</td>
</tr>
<tr>
<td>Other logistic support</td>
<td>0</td>
<td>5</td>
<td>250</td>
<td>100</td>
</tr>
<tr>
<td>Manufacturers NACE Group D*</td>
<td>2.5</td>
<td>36.075</td>
<td>10</td>
<td>28.200</td>
</tr>
<tr>
<td>Construction NACE Group E**</td>
<td></td>
<td></td>
<td>10</td>
<td>2,000</td>
</tr>
</tbody>
</table>

Total: 37,055

Figure 6.2: Percentage of enterprises not included in the assessment

This leaves the number of companies on which the total cost calculation is based and which need to respond in the years to come to legislation, as recommended in this report, in the range as indicated in Figure 6.3. (Companies meeting other security requirements also need to respond to the legislation but already do so through mutual recognition)

**Number of enterprises in the EU 25, affected by EU legislation only.**

<table>
<thead>
<tr>
<th></th>
<th>Micro &lt;10 empl.</th>
<th>Small &lt;50 empl.</th>
<th>Medium &lt;250 empl.</th>
<th>Large &gt;250 empl.</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail repair/maintenance shops</td>
<td>1,500</td>
<td>1,000</td>
<td></td>
<td></td>
<td>2,500</td>
</tr>
<tr>
<td>Road transport</td>
<td>450,000</td>
<td>47,500</td>
<td>2,250</td>
<td>150</td>
<td>499,900</td>
</tr>
<tr>
<td>Rail transport</td>
<td>6</td>
<td>18</td>
<td></td>
<td></td>
<td>24</td>
</tr>
<tr>
<td>Inland shipping</td>
<td>7,470</td>
<td>150</td>
<td></td>
<td></td>
<td>7,620</td>
</tr>
<tr>
<td>Warehousing</td>
<td>2,850</td>
<td>21,600</td>
<td>750</td>
<td></td>
<td>25,200</td>
</tr>
<tr>
<td>Other logistic support</td>
<td>54,000</td>
<td>4,750</td>
<td>900</td>
<td></td>
<td>59,650</td>
</tr>
<tr>
<td><strong>Total logistic sector</strong></td>
<td><strong>514,320</strong></td>
<td><strong>75,500</strong></td>
<td><strong>4,906</strong></td>
<td><strong>168</strong></td>
<td><strong>594,894</strong></td>
</tr>
<tr>
<td>Manufacturers NACE Group D</td>
<td>1,406,925</td>
<td>253,800</td>
<td>36,000</td>
<td>3,400</td>
<td>1,700,125</td>
</tr>
<tr>
<td>Construction NACE Group E</td>
<td>2,250,000</td>
<td>62,000</td>
<td>18,000</td>
<td>1,000</td>
<td>2,331,000</td>
</tr>
</tbody>
</table>

**Totals**

4,171,245 391,300 58,906 4,568 4,626,019

Figure 6.3: Number of companies that need to respond to intra-EU supply chain security requirements

**6.1.2 Cost per company**

For each specific supply chain security measure, as defined in figure 4.4 per industry group and per company size the cost have been assessed which will be incurred by the affected participants of the intra EU supply chain, both for implementation of security management as well as for annual maintenance. Overview of the cost assessment is included in Appendix D.
In making this cost assessment it is assumed that only very few companies have none of the measures as specified in Figure 4.4 in place. Much of these requirements are common sense and most companies will have some ad-hoc measures in place to protect their property. A summary of the investment and annual cost, based on appendix D, for the different categories and sizes of companies is given in Figure 6.4.

### Cost per company in 1000 €

<table>
<thead>
<tr>
<th></th>
<th>Investment</th>
<th>Annual cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro</td>
<td>Small</td>
</tr>
<tr>
<td>Rail repair/maintenance shops</td>
<td>63</td>
<td>139</td>
</tr>
<tr>
<td>Road transport</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Rail transport</td>
<td>67</td>
<td>194</td>
</tr>
<tr>
<td>Inland shipping</td>
<td>8</td>
<td>47</td>
</tr>
<tr>
<td>Warehousing</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Other logistic support</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Manufacturers NACE Group D</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Construction NACE Group E</td>
<td>5</td>
<td>56</td>
</tr>
<tr>
<td>Weighted average</td>
<td>5</td>
<td>50</td>
</tr>
</tbody>
</table>

Manuf. Sec. cost in % of turnover: 0.5, 1.1, 0.6, 0.4, 0.3, 0.8, 0.6, 0.4

Figure 6.4: Cost for implementing and annual maintenance of security management

It should be noted that both the implementation and the annual cost (in relation to the turnover) for small enterprises, are considerably higher than for the other assessed categories. Whereas micro companies due to their simplicity can achieve compliance with the proposed requirements by simple inexpensive means, small companies between 10 and 50 employees get to a size and a degree of complexity that the measures they need to implement to secure their operations are becoming more costly, whilst their turnover is still fairly moderate. (specification of the costs are included in Appendix D)

Besides it is assumed that the cost for especially micro enterprises can be kept at the assumed low level when industry associations are willing to develop simplified common instruments which companies can implement. A good example of this is the toolkit which IRU has developed for the road transportation sector.

It should be noted that the cost for inland shipping is relatively high, especially when one considers the fact that most inland waterway companies are 2 to 3 man companies. The reason however is that inland berthing places for barges are poorly protected and makes inland shipping quite vulnerable. However, in contrast, the necessity for enhanced security levels is far from necessary for a substantial volume of the conventional bulk market (sand, etc)

Due to the chosen methodology, which places emphasis on “normal” and location bound companies, the investment and annual costs defined for rail companies in figure 6.4 are disproportionately low, considering the complexity of their operations. Rail transport companies are extra vulnerable to terrorist attacks because they generally use long trains which are easy accessible and which have fixed routes making them very predictable. Furthermore the rail transport companies cover large distances requiring geographical spread of the security measures. In reality rail transport companies therefore need to invest a multitude of the amount specified in figure 6.4.
The drafted security measures are a combination of hardware, system and organisational measures. The hardware measures tend to have high investment cost compared to their annual cost, the organisational measures tend have high annual cost compared to their investment cost and the system cost are somewhere in between.

Through the mix of security measures, the investment costs required for implementing security management tally up to be approximately equal to the annual cost, as can be seen in figure 6.4. Therefore when spread over a period of 10 years, the investments costs only form 10% of the annual costs. Another approach is to calculate the complete investment costs as the first year costs, while the annual costs are calculated from the second year on. This would mean that the investment costs need to be recuperated in one year, which needs to be viable since subsequent annual costs, are of the same order.

6.1.3 Total cost for industry in mandatory scheme

Figure 6.5 specifies the total cost for trade and industry for mandatory implementation of security management in the supply chains within the EU 25. The data is obtained through the multiplication of the number of companies as specified in figure 6.3 with the cost per company as specified in figure 6.4. No correction has been made for the expected higher costs for rail transportation companies. However, considering the limited number of rail transport companies their effect on the total costs would also be negligible.

<table>
<thead>
<tr>
<th></th>
<th>Investment</th>
<th>Total</th>
<th>Annual cost</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail repair/maintenance shops</td>
<td>0</td>
<td>95</td>
<td>139</td>
<td>0</td>
</tr>
<tr>
<td>Road transport</td>
<td>1.215</td>
<td>570</td>
<td>110</td>
<td>22</td>
</tr>
<tr>
<td>Rail transport</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Inland shipping</td>
<td>60</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Warehousing</td>
<td>14</td>
<td>1.210</td>
<td>97</td>
<td>0</td>
</tr>
<tr>
<td>Other logistic support</td>
<td>111</td>
<td>90</td>
<td>39</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total logistic sector</strong></td>
<td><strong>1.400</strong></td>
<td><strong>1.972</strong></td>
<td><strong>385</strong></td>
<td><strong>25</strong></td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>19.685</strong></td>
<td><strong>19.657</strong></td>
<td><strong>7.945</strong></td>
<td><strong>1.371</strong></td>
</tr>
</tbody>
</table>

Figure 6.5: Total cost to industry for implementing and maintaining security management

Both the total required investment and the annual cost which European trade and industry shall absorb in order to comply with the legislation as proposed in this report are in the order of 40 to 50 Billion Euro, which is less than 0.5% of the Unions annual GDP. This means that the initial investment costs when calculated over a reasonable period of time (e.g. ten years) becomes negligible on an annual basis.

It is arguable that the mutual recognition between security regimes cannot be arranged before the mandatory deadline of 2009. In that case all operators in the supply chain will be required to comply with the supply chain security requirements as defined in this report, resulting in the costs as calculated in figure 6.6.
It is interesting to see, given the relation which exists between the production-value of manufacturers and the quantity of goods which they bring into the supply chain, that an analysis shows that around 60% of the supply chain is initiated by large enterprises, whilst micro enterprises, in spite of their large number, only contributes with 6%.

| Micro company | 4,208,300 | € 5,000 | € 21 billion |
| Small company  | 424,800  | € 50,000 | € 21 billion |
| Medium company | 98,008   | € 135,000 | € 13 billion |
| Large company  | 19,335   | € 300,000 | € 5 billion  |
| **Total**      | **4,750,443** |  | € 60 billion |

Reliable statistics on how the enterprises in figure 6.5 are geographically spread are not available.

6.1.4 Total cost for industry if requirements remain voluntary

As discussed in chapter 5, the implementation of the supply chain security requirements should initially follow a voluntary roll out program after which in 2009 it is made mandatory for all supply chain participants. The above calculations are based on the mandatory situation where all participants comply.

Even though this study recommends the eventual mandatory implementation of the program, the cost impact of keeping the program voluntary is also calculated below.

The percentage of participating companies in a voluntary scheme is determined using the following “motivating” criteria:

1) **Brand reputation**: Possible brand damage a company may suffer in case it is involved in a terrorist attack. Resulting in loss of business and revenue.

2) **Anti theft and vandalism**: Implementation of security measures to protect against terrorist interventions also secures the supply chain and its cargo against theft and vandalism. Operators responsible for the cargo will experience a reduction in losses. Manufacturers will reduce market competition of stolen goods which are introduced on the market at bargain prices.

3) **Brand profile (business to business)**: Implementation of security measures creates positive brand profiling in business to business relationships. Operators can present themselves as resilient organisations and reliable partners. Implementation of security management can guarantee a license to operate in secure supply chains.

4) **Green lane**: Secure operators will enjoy preferential treatment through facilitation and simplification of security control measures during inspections.

5) **Social responsibility**: Implementation of security management in the organisation can positively contribute to an organisation’s social responsibility policy.
6) **Cost:** The cost of implementing security management in the organisation (in relation to turnover) should be considered as a inverse motivator.

The influence of each criteria on both the type and the size of company has been determined.

In the table below the number of companies is given that will participate in a voluntary scheme, grouped in the following categories:

- **Shippers** represent the manufactures, construction and the rail repair/maintenance shops
- **Transporters** represent road transport, rail transport and inland shipping
- **Forwarders** represent the other logistic support
- **Terminal operators** represent warehousing and conventional terminals.

![Table of participation in a voluntary program](image)

<table>
<thead>
<tr>
<th>MICRO</th>
<th>SMALL</th>
<th>MEDIUM</th>
<th>LARGE</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td># comp.</td>
<td>% particip.</td>
<td># particip.</td>
<td># comp.</td>
<td>% particip.</td>
</tr>
<tr>
<td>SHIPPERS</td>
<td>365300</td>
<td>15</td>
<td>533950</td>
<td>25</td>
</tr>
<tr>
<td>TRANSPORTERS</td>
<td>458300</td>
<td>30</td>
<td>137490</td>
<td>50</td>
</tr>
<tr>
<td>FORWARDERS</td>
<td>54000</td>
<td>20</td>
<td>10800</td>
<td>50</td>
</tr>
<tr>
<td>TERMINAL OPERATORS</td>
<td>3000</td>
<td>10</td>
<td>300</td>
<td>24000</td>
</tr>
</tbody>
</table>

**Figure 6.7: Participation in a voluntary program**

Divided per group of operators:

- **Shippers,** 718.825 companies (17%);
- **Transporters,** 165.365 companies (32%);
- **Forwarders,** 12.050 companies (20%);
- **Terminal operators,** 8.300 companies (30%).

The above participation values are including the companies already covered by other security requirements as discussed in figure 6.2. When these companies are deducted and the remaining numbers are multiplied by the average investment cost per company size the following overview is produced:

![Table of costs](image)

| Micro company | 665.485 | € 5,000 | € 3.3 billion |
| Small company | 86.225 | € 50,000 | € 4.3 billion |
| Medium company | 24.805 | € 135,000 | € 3.4 billion |
| Large company | 3.601 | € 300,000 | € 1.1 billion |
| Total | 776.440 | € 12.1 billion |

**Figure 6.8: Cost of a voluntary program**

Considering in the mandatory calculation the annual costs are near equal to the investment cost, a similar equality can be expected for the voluntary calculation.
6.2 The cost to Member States for implementing legislation

Whereas there is broad consensus that the security of the supply chain of intra EU cargo traffic shall be improved, and it is concluded above that this does not create unacceptable expenses for industry, an assessment has been made of the cost this would have for the EU and the Member States.

6.2.1 Implementation of security management throughout the supply chain

The cost for implementation is caused by 2 aspects.

a.) Ensuring the implementation of security management by industry.

It is recommended that the Member States motivate the leading industrial enterprises to start implementing security management in their supply chain by:

- Explaining that security management requirements will become compulsory in the coming years.
- Explaining that compliance to requirements will provide them with a green lane.
- Explain the other benefits as spelled out in this report.
- Appeal on their social accountability and industrial responsibility.

and they should ensure that these leading companies start enforcing security requirements on the partners they have in the supply chains they manage.

A major multinational manufacturer of consumer and industrial electronics with 300,000 employees in 300 plants, spread all over the world has corporate wide implemented security management to its own standard. Their motivation was to reduce the number of inspections at customs (in the US they succeeded to reduce these with 90%) and to avoid brand damage.

The investment needed for this was estimated to be between 100,000€ and 500,000€ per plant. Apart from reduced inspections it was considered still to be too early to measure the benefits yet. A general impression however is that only in a few locations where major investments in hardware had to be made the investments exceeded the immediate benefits.

All plants are subject to a periodic audit system and also subcontractors are audited for compliance to the companies own security standard (elements of the subcontractors operation with no relevance to the subcontract are not included in these audits)

This will create a momentum and increased awareness which at least will ensure compliance of the more responsible operators in the supply chain. During the first years this is not an expensive effort and can be managed by existing resources, both at the commission and in the Member States and therefore is cost neutral.

It is however essential that the legislation is going to be enforced on all operators in the not too far future. (Ideally the deadline for implementing the legislation on all operators in the supply chain should be the same as the implementation of the revised customs code of the union, but 2009 may be a bit late)

From that point onwards the Member States need to cover the possible cost for verifying implementation (b. below) and the cost for enforcement (6.2.2 below).
b.) Verifying implementation through audit

This report recommends that verification if the requirements of the legislation are properly implemented in all relevant organisations should either be through audits by (newly to establish) inspectorates within the Member States, delegation of these audits to RSO’s or to accredited 3rd party certification bodies. Initial audits should be performed to verify compliance and annual audits should be performed to ensure that systems remain effective.

As one of the major international certification bodies DNV has the experience that these periodic audits are essential in the prevention that management systems are slipping away. Reality shows that only very few companies have the capability and convincing policies which prevent that management quickly dilute. DNV recommends that periodic audits need to be performed annually to ensure that changes in organisations and their business environment are adequately followed up by adaptation of the security management program.

To determine total cost for an audit scheme covering the whole EU, the auditing cost per company has been assessed together with the assessment of the cost for industry for implementing security management (see appendix D, last cost row per company type). The assessment of the auditing cost per company is based on 600 to 800 euros per audit day and the number of audit days required taking into account the size of companies (based on DNV’s auditing experience). Accordingly, the auditing cost per company has been multiplied by the number of companies from figure 6.3 to obtain a total figure covering the whole industry. A total of 4.626.019 companies are covered in the calculated audit scheme below.

### Cost for initial and annual verification of compliance (auditing) in million €

<table>
<thead>
<tr>
<th></th>
<th>Initial Cost</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Annual Cost</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail repair/maintenance shops</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>259</td>
<td>97</td>
<td>15</td>
<td>1</td>
<td>371</td>
<td>103</td>
<td>75</td>
</tr>
<tr>
<td>Road transport</td>
<td>225</td>
<td>48</td>
<td>7</td>
<td>1</td>
<td>280</td>
<td>90</td>
<td>48</td>
<td>2</td>
<td>0</td>
<td>140</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rail transport</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inland shipping</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warehousing</td>
<td>3</td>
<td>43</td>
<td>2</td>
<td>0</td>
<td>48</td>
<td>1</td>
<td>22</td>
<td>1</td>
<td>0</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other logistic support</td>
<td>27</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>34</td>
<td>11</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total logistic sector</strong></td>
<td><strong>259</strong></td>
<td><strong>97</strong></td>
<td><strong>15</strong></td>
<td><strong>1</strong></td>
<td><strong>371</strong></td>
<td><strong>103</strong></td>
<td><strong>75</strong></td>
<td><strong>5</strong></td>
<td><strong>183</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturers NACE Group D</td>
<td>703</td>
<td>254</td>
<td>108</td>
<td>17</td>
<td>1.082</td>
<td>281</td>
<td>152</td>
<td>36</td>
<td>7</td>
<td>476</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction NACE Group E</td>
<td>1.125</td>
<td>62</td>
<td>54</td>
<td>5</td>
<td>1.246</td>
<td>450</td>
<td>37</td>
<td>18</td>
<td>2</td>
<td>507</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>2.087</strong></td>
<td><strong>413</strong></td>
<td><strong>177</strong></td>
<td><strong>23</strong></td>
<td><strong>2.700</strong></td>
<td><strong>834</strong></td>
<td><strong>264</strong></td>
<td><strong>59</strong></td>
<td><strong>9</strong></td>
<td><strong>1.167</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6.9 Cost for auditing.

These figures are based on the assumption that Member States delegate these tasks to RSO’s or accredited 3rd party certification bodies. Whereas these companies have a standing organisation, either they already certify against the ISPS code or the ISO management system standards they need minor investments in additional training to adapt to these new roles.

Where Member States decide to nominate RSO’s they should account for 0,2 to 2 man-years (depending the size of their economy) to ensure that the RSO’s operate at the desired quality level. The certification costs are absorbed by industry.
Where they decide to delegate the verification to accredited 3rd party certification bodies both accreditation and certification costs are absorbed by industry. Apart from a minor investment for formulating the criteria which the accreditation bodies shall apply this approach is cost-neutral to the Member States. This would be the most cost-effective solution for the Member States.

When Member States decide to establish new inspectorates to perform these verifications the start-up and the maintenance of a new organisation in one of their public bodies is anticipated to be 20% more expensive than when these verifications are delegated to existing commercial certification organisations.

Based on the distribution of the number of employees employed (in the defined industry sectors, see section 6.1) across the 25 Member States, the cost per individual Member State is calculated. The relative number of employees are assumed to be a representative value for the relative number of companies present in each Member State and thus the distribution of the auditing costs.

<table>
<thead>
<tr>
<th>Inhabitants (X 1000)</th>
<th>number of employees (X 1000)</th>
<th>Auditing cost initial (M€)</th>
<th>Auditing cost annual (M€)</th>
<th>Cost for enforcement (M€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>8.140</td>
<td>731</td>
<td>52</td>
<td>23</td>
</tr>
<tr>
<td>Belgium</td>
<td>10.396</td>
<td>784</td>
<td>56</td>
<td>24</td>
</tr>
<tr>
<td>Cyprus</td>
<td>730</td>
<td>32</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>10.212</td>
<td>1.397</td>
<td>100</td>
<td>43</td>
</tr>
<tr>
<td>Denmark</td>
<td>5.398</td>
<td>543</td>
<td>39</td>
<td>17</td>
</tr>
<tr>
<td>Estonia</td>
<td>1.351</td>
<td>156</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>Finland</td>
<td>5.220</td>
<td>498</td>
<td>36</td>
<td>15</td>
</tr>
<tr>
<td>France</td>
<td>59.901</td>
<td>4.738</td>
<td>338</td>
<td>146</td>
</tr>
<tr>
<td>Germany</td>
<td>82.532</td>
<td>8.250</td>
<td>589</td>
<td>255</td>
</tr>
<tr>
<td>Greece</td>
<td>11.041</td>
<td>506</td>
<td>36</td>
<td>16</td>
</tr>
<tr>
<td>Hungary</td>
<td>10.117</td>
<td>968</td>
<td>69</td>
<td>30</td>
</tr>
<tr>
<td>Ireland</td>
<td>4.028</td>
<td>284</td>
<td>20</td>
<td>9</td>
</tr>
<tr>
<td>Italy</td>
<td>57.888</td>
<td>4.705</td>
<td>336</td>
<td>145</td>
</tr>
<tr>
<td>Latvia</td>
<td>2.319</td>
<td>192</td>
<td>14</td>
<td>6</td>
</tr>
<tr>
<td>Lithuania</td>
<td>3.446</td>
<td>289</td>
<td>21</td>
<td>9</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>452</td>
<td>45</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Malta</td>
<td>400</td>
<td>30</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands</td>
<td>16.258</td>
<td>1.084</td>
<td>77</td>
<td>33</td>
</tr>
<tr>
<td>Poland</td>
<td>38.191</td>
<td>2.553</td>
<td>182</td>
<td>79</td>
</tr>
<tr>
<td>Portugal</td>
<td>10.475</td>
<td>948</td>
<td>68</td>
<td>29</td>
</tr>
<tr>
<td>Slovakia</td>
<td>5.380</td>
<td>464</td>
<td>33</td>
<td>14</td>
</tr>
<tr>
<td>Slovenia</td>
<td>1.996</td>
<td>301</td>
<td>22</td>
<td>9</td>
</tr>
<tr>
<td>Spain</td>
<td>42.345</td>
<td>2.985</td>
<td>213</td>
<td>92</td>
</tr>
<tr>
<td>Sweden</td>
<td>8.976</td>
<td>881</td>
<td>63</td>
<td>27</td>
</tr>
<tr>
<td>UK</td>
<td>59.673</td>
<td>4.448</td>
<td>318</td>
<td>137</td>
</tr>
</tbody>
</table>

456.865  37.812  2.700  1.167  450

Figure 6.10: Distribution over the Member States of cost for auditing and enforcing compliance
Auditing costs for Member States if requirements remain voluntary
If it is decided, as discussed in section 6.1.4, to keep the program voluntary after 2009, the aud-iting costs will turn out much lower for the Member States. Using the voluntary participation figures from figure 6.7 minus the already participating figures from figure 6.2 and the auditing cost per company, as defined in Appendix D, the auditing cost in a voluntary program are calculated as presented in figure 6.11. A total of 776,440 companies are included in the audit scheme below.

<table>
<thead>
<tr>
<th>in M€</th>
<th>Initial cost</th>
<th>Annual cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro Small Medium Large</td>
<td>Total</td>
</tr>
<tr>
<td>Shippers</td>
<td>257 58 67 17</td>
<td>400</td>
</tr>
<tr>
<td>Transporters</td>
<td>68 23 5,0 0,8</td>
<td>97</td>
</tr>
<tr>
<td>Forwarders</td>
<td>5,4 0,8 0,5 0,0</td>
<td>7</td>
</tr>
<tr>
<td>Terminal operators</td>
<td>0,15 10 1,7 0,0</td>
<td>11</td>
</tr>
</tbody>
</table>

Figure 6.11: Auditing costs under a voluntary program

The 514 M€ initial audit costs need to spread over the estimated years required to achieve the defined participation levels. The annual costs of 227 M€ will gradually build up until the defined participation levels are realised.

The audit costs for the ‘large’ companies are relatively low because it is estimated that a large number of those companies will already comply with existing security requirements, meaning that only a small number will need to be audited under supply chain security requirements.

6.2.2 Enforcement
Initial audits are recommended to ensure the implementation of security management and to verify compliance to the requirements. Only after successful initial audit will an operator receive a secure status. Consequently annual periodic audits are recommended to ensure maintenance of the system and verify continual effectiveness of the system. While the periodic audits should also ensure continuous compliance to the requirements, they need to be backed up by spot check inspections as an additional enforcement tool.

As discussed in section 5.2.2.3 and figure 5.4 a distinction can be made in the functionality of the enforcement program during the voluntary roll out phase and the mandatory phase.

Voluntary roll out phase
During the voluntary phase the inspection program has a dual objective. First of all it needs to enforce the compliance to the requirements for all operators participating in the supply chain security program. Secondly, it needs to create a level of scrutiny of the non-participating operators which would make ‘green lanes’ and thus participation attractive to them. Therefore, the number of inspections needs a sharp increase compared to present inspection levels in order to facilitate both objectives.

Based on the two objectives the following calculation is made of the enforcement costs during the voluntary roll out.

The number of trucks and lorries engaged in the supply chain within the EU is anticipated to be in the order of 2½ million. The amount of systematic safety related road checks by traffic po-
lice, traffic inspectorates and customs is in the order of 4% per annum amounting to approx 100,000 inspections of documentation, the vehicle and its cargo.

The current cost for enforcement of compliance to legislations regarding cargo traffic safety, social security and fiscal requirements hence amounts to approximately 25 million Euros per annum. For extending the inspections from ½ an hour per vehicle to ¾ of an hour to include compliance to security legislation and raising the number of inspections to 10% would increase the cost of inspections to a level of around 95 million Euros, an increase of 70 million Euros per year.

The expense to verify compliance of rail and shipping would be much less so the additional cost of enforcement of supply chain security management will be in the order of 80 to 100 million Euros per annum for the Member States.

Besides the number of companies which are not subjected to traffic inspections but also need to be verified (by labour safety or other directorates) like shippers, warehouses etc. is approx. 3.5 times the number of transport companies.

This brings the expense for enforcement by the Member States to an order of 400 to 500 million € p.a. during the voluntary roll out phase in order to both facilitate the ‘Green lane’ principle and enforce continuous compliance for the participating operators.

**Mandatory phase**

Once the supply chain security requirements become mandatory, the ‘green lane’ principle become obsolete and with it the large number of inspections. Spot check inspections only need to ensure continuous compliance as a safety under the periodic audits.

The assessment of the cost of enforcement in the mandatory phase is made under the assumption that the implementation and maintenance of supply chain security management is certified by government bodies or independent third parties and hence a reasonable level of confidence exists in the periodic audits.

Therefore, once the requirement for implementing security management in the supply chain has been completely implemented the amount for enforcement can be reduced towards the present level of around 50 Million Euro p.a.

If the requirements remain voluntary

In the case it is decided not to follow up the voluntary phase with mandatory phase, the inspection and enforcement costs will have to remain at the level of the voluntary roll out phase, in order to uphold the ‘green lane’ principle.

### 6.3 Other costs

The other costs are represented by the three remaining instruments. Costs can either be for industry, for Member States or for both, as will be discussed below.

#### 6.3.1 Awareness campaigns

Since the target group of EU driven awareness campaigns are workers in the supply chain no need exists to utilise the expensive communication channels of mass media. The campaigns should mainly work through professional magazines and industry organisations in order to mo-
bilise the management of organisations to raise awareness with their company staff. Since awareness is the key to successful security management the Member States and the commission should permanently dedicate staff to launch campaigns, develop tools and instruments to support industry in their endeavours and to manage possible special projects. The cost for this would not be more than one or two million Euro p.a. for the EU.

The cost for the execution of awareness campaigns within organisations are already included in the operational cost calculations for the implementation of security management (section 6.1).

6.3.2 The employee vetting system

Where it is recommended that the private sector will possibly establish and operate a database of vetted mobile employees there will be a cost incurred by this. Considering that there are between 2 and 2½ million truck drivers in the EU that will need to be vetted a reasonable assumption is that 15 to 20 % of them can be categorized as mobile (i.e. self employed, working for agencies or job-hoppers). An equal amount of warehouse workers from the same category can be assumed.

This brings the number of employees that will be stored in these databases in the order of 800,000.

Developing a secure database with internet access to the database will be minor investment compared to the day to day maintenance. However, if the database is maintained on a daily basis by Secure Economic Operators and/or specialised labour agencies in the EU the cost will be carried by those operators which also will reap the benefits of such database.

Assuming that mobile employees in average work for a period of 3 months for an employer and that a proper vetting costs ½ a day per employee a central data base of vetted employees would save the logistic industry around 800 million Euros, which by far outweighs the maintenance of such database.

This measure would be cost neutral to the Member States and the Commission. The operational cost of the vetting, required to be paid by the operators to the specialised labour agencies, are already covered by the operational costs calculated for implementing security management by the industry (section 6.1)

6.3.3 EU Seal programme

Goods for export to outside the EU have to be fitted with seals already. Intra EU traffic amounts to 2 billion tons per year. Assuming that 80% of this cargo is subject to the seal programme and an average cargo unit weighs 20 tons the number of seals needed to implement an EU seal program will be 80 million.

High security seals, compliant to ISO PAS 17712 have a cost of below 0.75 Euro a piece. Assuming that it takes 2 minutes to mount and dismount such a high security bolt the additional cost for industry would be in the order of 150 million Euros. These costs however will be outbalanced by the gains as specified and are already included in the operational cost calculation for implementing security management by industry (section 6.1)
This measure might require a very minor investment by the commission in the sense of establishing required standards, but would be cost neutral to the Member States.

6.4 Benefits to industry

6.4.1 Implementing security management

Primarily it is in the interest of the Member States that the proposed legislation is implemented since the direct effect of implementing security management as proposed by this report is that it reduces the likelihood that the logistic system within the EU is utilised to perform terrorist related crime of which the consequences can be enormous in terms of lives lost and economic damage. Besides implementing security management will increase the transparency of the supply chain which will facilitate improved risk assessment by the law enforcement authorities.

A recent study has assessed that detonating a 10-20 KTon nuclear device in a container terminal may cause an economic damage of €150-700 Billion and 50,000 to 1,000,000 casualties. (Abt Associates)

Since the cost for security management however is mainly carried by the industry it is important to see if implementing security management in an organisation brings that company collateral benefits.

- Sustainability and resilience of organisations.
- Trade facilitation
  - Reduced number of cargo inspections
  - Level playing field.
- Reduction of theft of cargo.
- Preventing damage to brand and reputation.
- Increased efficiency and transparency.

An assessment of these side effects has been made, resulting in the estimated benefits as specified below. However it must be recognised that a quantitative assessment is difficult to achieve for things which have not yet occurred, where no historic reference is applicable and for which no statistical supporting data is available. Therefore, the assessments, where possible can only be based on qualitative analysis supported by broad estimates.

**Sustainability and resilience of organisations**

In an industrialised environment where just-in-time management and outsourcing are the cornerstones of today’s industry the dependency of industry on reliable supply chains is crucial. It is anticipated that terrorists are able to disrupt supply chains to a degree and for a period that the existence of individual companies can be endangered.

Of course it is impossible to quantify the consequences of events that did not yet happen, but it is evident that a more secure supply chain reduces the economic vulnerability of trade and industry to terrorist interventions and increases their ability to recover when a terrorist intervention does happen.
Trade facilitation
Where multinational corporations or large exporters increasingly are going to seek Secure Operator status in line with the recommendations of this report or Approved Economic Operator status with customs (Ref is made Appendix C) in order to reduce authorities intervening in their supply chain they take on board the responsibility to ensure that all parties in the supply chains under their control are secure operators.

This will not only reduce the amount of cargo inspections which Secure Operators are subject to, through the proposed green lane principles, but also cause that implementation of security management with service suppliers to these large organisations becomes a commercial advantage.

Furthermore, common minimum security standards will ensure a level playing field. Commercial advantages due to deviations in national security requirements between Member States is not possible, since operators must meet the same requirements in all Member States.

Reduction of cargo theft.
Whereas the majority of the security measures, as specified in Figure 4.4 have the objective to prevent that cargo can be accessed by unauthorised persons or, if this happens, an alarm is being raised it is self-evident that preventing unauthorised access to cargo also will reduce the theft of cargo.

It however is hard to obtain accurate data about cargo crime, reliable statistics about cargo theft within the EU do not exist. Data is fragmented and for many Member States non existent. A study made in the US, however, shows that the FBI estimates annual cargo theft in the US alone to be in the order of $18 Billion. The Department of Transportations estimate is that, including administrative costs cargo thefts costs US economy $20 to $60 Billion p.a.

Michael Wolfe has analysed that not only as little as 40 percent of cargo theft is reported to the authorities, but also that stolen goods will appear on the market at a much lower price than originally intended. Besides there are added expenses for reshipment of the stolen goods, disrupted customer relation and brand damage to be added, which results in an estimated cost to the US economy of well over a $100 billion per annum. Where the economies of the US and the EU in terms of GDP are equal it is not unrealistic that the cost of cargo theft in the EU is in the same order of magnitude.

If a conservative assumption is made that a broad implementation of security management throughout the supply chain would reduce cargo theft with 10% this would imply a benefit for European economy of 10 billion €.

It should be noted however that this benefit is not evenly distributed over all operators in the supply chain. Only those parties which hold ownership of or liability for the cargo (shippers, warehouses and to some extend transporters) reap the benefit in terms of reduced losses and

---

8 Ref. the journal of commerce July 26-August 1 2004 by Michael Wolfe
insurance premiums. Other parties, like for instance freight forwarders, agents etc. do not have these benefits.

**Preventing damage to brand and reputation**

Brand risk is the threatened loss of value due to a change in people’s perceptions about a company. Loss of brand reputation may have dramatic consequences for a company.

---

*Over a five-year span, 10% of the Fortune 1,000 companies lost 25% of their market value in four weeks or less. Their losses were due to brand-related causes. This represents a loss in the order of 250 Billion €. Brand damage is one of the major business risks of the 21st century. Product incidents -- recalls, boycotts, scandals -- can cost companies billions, affect share prices and even result in bankruptcies*

---

Large corporations fear that if their name gets connected to terrorism this will have a negative effect on their sales since consumers will get stuck with a negative perception. Especially the supply chain, with all its vulnerabilities, represents a serious brand risk to these companies. If the message gets out in the media that in a container loaded with HP-computers also terrorist weapons were found this would represent a serious kick back in the market for HP.

However also service companies in the supply chain, from which it becomes known that they had security lapses which resulted in a terrorist incident will find them in an extremely difficult market situation.

On the other hand, when companies can demonstrate that they have a safe and secure performance this will be appreciated by the market as a premium, and hence becomes a commercial advantage.

**Increased efficiency and transparency**

Implementing Security Management in the supply chain in a systematic manner will increase efficiency and transparency of the logistic sector.

If the same approach is taken as in quality management, environmental management and (food) safety management and companies commit themselves seriously to implement security management system the investment they need to make will be paid back in multifold.

Whereas the prime objective of the existing management system standards have been to improve the quality and environmental performance of organisations the systematic analyses of their processes and the requirements for continuous improvement have created unexpected pleasant side effects for organisations. Also their financial performance improved, in spite that industry representatives tend to complaint that management system increase bureaucracy and raise cost, especially when they are implemented under regulatory requirements. This over the years has proven to be more based on resistance to change than actual facts.
In order to make an assessment of the benefits it is best to draw a parallel with the effects implementation of the ISO 9000 standard had on industry. (That there exists a very large similarity between the consequences of implementing security management and quality management in the supply chain is extensively demonstrated by Hau L. Lee and Michael Wolfe\textsuperscript{9} which underpin the view that a systematic approach to security enhances the efficiency of the supply chain)

### Implementation ISO 9000

At present 700,000 organisations have been certified globally against the ISO 9000 standard and a study by Corbett et all\textsuperscript{10} has demonstrated how big efficiency gains are. This study is comparing the performance data of ISO 9000-certified companies in three US business sectors over a 10-year period (1988-1997) against that of reference groups of non-certified firms in the same sectors. Companies which had a comparable business performance, prior to the launching of ISO 9000 programs by the certified companies, showed a considerable increase of their Return On Assets (ROA), compared to the reference groups. After they started the implementation of their systems, for the chemical sector this increase was almost 20% and the ROA of 2 manufacturing sectors more than doubled that of the reference groups over the five years period.

<table>
<thead>
<tr>
<th>Year</th>
<th>ROA (%) Chemical</th>
<th>ROA (%) Mechanical</th>
<th>ROA (%) Electronic</th>
</tr>
</thead>
<tbody>
<tr>
<td>t-2</td>
<td>10</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>t-1</td>
<td>11</td>
<td>16</td>
<td>13</td>
</tr>
<tr>
<td>t</td>
<td>12</td>
<td>17</td>
<td>14</td>
</tr>
<tr>
<td>t+1</td>
<td>13</td>
<td>18</td>
<td>15</td>
</tr>
<tr>
<td>t+2</td>
<td>14</td>
<td>19</td>
<td>16</td>
</tr>
<tr>
<td>t+3</td>
<td>15</td>
<td>20</td>
<td>17</td>
</tr>
</tbody>
</table>

\textsuperscript{9} \textit{Ref.} Supply Chain management Review - January/February 2003 Supply chain Security Without tears

\textsuperscript{10} \textit{Ref.} ISO Management Systems magazine – July-August 2002 by David A. Kirsch, María José, Alvarez-Gil, Charles J. Corbett and María J. Montes,

Considering that the total asset value of the industry sectors which are effected by the proposed legislation is well over 10 Trillion €, as little as 0.4 % gain in efficiency due to a more systematic approach to security management would counterbalance the investment and annual cost which industry has to spend.
The balance for industry
Apart from the improved security of the supply chain in general it can be concluded that for the whole logistic sector in the EU the cost for implementing security management will be well out-weighed by the material benefits, if measures are based on a proper risk assessment and are appropriate to the size and type of the operation.

Whereas the cost are distributed over all parties in the supply chain the benefits in terms of reduction in theft are fostered however only by those parties which hold liability for the integrity of the cargo. This means that implementing security management in the intra European supply chain will lead to a minor shift in cost from the shippers and cargo owners to service providers which do not have direct contact with the cargo.

6.4.2 Audit: verification of implementation
The implementation of a common European wide audit scheme to verify implementation benefits the industry with:
  - a level playing field;
  - prevention of multiple audits;
  - assignment of secure operator label.

Common auditing criteria and procedures will be defined for the whole EU, ensuring that international competition is not disrupted because of unequal security requirements because of different interpretation or execution by the different Member States. Level playing field will be guaranteed for the industry.

One common auditing scheme throughout the EU will also allow mutual recognition of one Member State’s findings by other Member States and customs. A company audited in one Member State is recognised as secure operator in all Member States. Multiple audits in the various countries in which the company operates will not be necessary.

Each audited company receives a secure operator label. Such a label allows the company to enjoy other benefits such as the green lane treatment and positive brand promotion (see previous section). These benefits can only be enjoyed if it can prove its compliance with the requirements.

6.4.3 Awareness programs
Implementation of awareness programs benefits the industry in two ways.

First of all the creation of security awareness among the employees supports effective implementation of security management and the security requirements into the organisation. Awareness positively influences human behaviour into more secure habits and social patterns.

Second, employee awareness directly contributes to securing the organisation against terrorist attacks through their participation in identifying and reporting suspicious behaviour.

6.4.4 Employee vetting system
In an European employee vetting programme employees with short term and unstable work relationships and who seek employment throughout Europe are vetted in a common program.
Positive screening results in a proof of vetting with which they are exempt from employer vetting when applying for jobs.

The main benefit of such a program is the creation of mutual recognition of screened employees. An employee vetted under the program is mutually recognised by all companies throughout the EU, preventing multiple vetting of a single employee when he or she changes employers times.

In section 6.3 the possible savings have been calculated to the order of € 800 million. With the assumption of 800,000 participating employees who under normal circumstances would require 4 screenings in a year, each with a duration of ½ day.

6.4.5 European seal programme
The benefit of a European seal programme to the industry is quick and simple. Application of seals allows easy inspection of whether the cargo has been accessed or not, reducing the amount of inspection time when a possible breach is suspected.

6.5 The benefits for Member States

6.5.1 Implementation of supply chain security management
Reduced risk of casualties and economic damage
Whereas the EU has defined security as one of its priorities the main benefit for the Member States of implementation of the proposed legislation is that the security of the supply chain is drastically increased. This means that the chance of massive casualties under their citizens or enormous damage to their economies, as calculated in the risk assessment in chapter 2, is reduced.

One approach throughout the EU
When the legislation is implemented similarly and simultaneously by all Member States, it is ensured that no single country sustains commercial advantages or disadvantages compared to other Member States and that their enterprises within the Union operate on a level playing field.

Provided the legislation is based on the recommendations of this report it will formulate requirements which are based on a thorough risk analysis of the potential hazards in the intra EU supply chain. This will avoid as much as possible knee-jerk reactions of the individual Member States which might disturb the level playing field for single countries’ enterprises.

The legislation will ensure that supply chain security management throughout the union is harmonised to an extend that recognition of companies as being secure operators can be acknowledged and accepted by the other Member States.

Increased confidence
Equally the legislation will formulate requirements which ensure that supply chains within the Union are having the same level of security as cargo traffic by road, rail, air and sea, crossing the outside borders of Europe.
Besides the legislation avoids as much as possible the development of large bureaucratic organisations and reduces red tape to the minimum.

6.5.2 Audit: verification of implementation

The application of an audit scheme ensures but also verifies not only that operators implement the security requirements but also implement them correctly. Those operators which correctly comply with the requirements receive a secure operator label by which they can be recognised.

It will not be possible for operators to proclaim themselves as being secure operators without being verified by the Member States.

With use of the secure operator label secure operators can identify themselves at security control inspections allowing them to make use of the green lane and pass the inspection without any delay. This allows the inspection services to focus on those operators which are not secure operators and thus improving the effective allocation of resources.

A mutually recognised secure operator label throughout the Member States increases the predictability for both the operators and the Member States. Member States can trust on the fact that an operator from another Member States must meet the same requirements and is audited on the same criteria with same procedures as its own. The security level is therefore never compromised. However, in order to maintain the level of confidence that operators maintain proper implementation of the requirements, periodic re-audits are necessary.

The application of an audit scheme with secure operator labels allows interconnectivity with other security requirements such as the airline security requirements and their ‘known consignor’ label and the custom security requirements and the ‘authorised economic operator’ label. Labels from the other security requirements can be mutually recognised.

6.5.3 Enforcement

While the audit scheme ensures the correct implementation of the security requirements, an enforcement scheme, based on spot check inspections, is required to ensure the continual compliance after the secure operator label has been awarded.

While the main goal of the enforcement scheme is to verify continued implementation, it will also contribute to verification of the effectiveness of the security management systems and measures and resolve any incorrect implementation/application of measures which might damage the effectiveness.

6.5.4 Awareness programs

Awareness programs contribute the continued awareness about the risks incurred by the supply chain and the need for compliance to security regulations and systems. It will stimulate operators to implement the security requirements and participate in the supply chain security scheme.

6.5.5 European seal programme

Is conditional for during security control inspections to verify if security has been violated en route.
7.0 Conclusions & Recommendations

7.1 Conclusions

It is imminent that terrorists, in order to realise their objectives, may need to utilise the supply chain, either to transport their malicious goods or by utilising the (stored) energy to cause devastation, either in terms of fatalities or as damage to the economy, whereas the threat that terrorist are targeting one of the European Member States is increasing.

To anticipate on this threat
- The security of cargo transportation by air and by sea is by now well regulated and adequate measures are implemented.
- The security of import and export of goods into and out of the union is ensured by customs inspections and will further be improved after the implementation of the Revised Customs Code.
- The security of transports of dangerous goods along the European transportation infrastructure is drastically improved to an acceptable level after the recent update of the ADR regulations.

Since any chain is as weak as its weakest link, not addressing security of the supply chains within the union these measures are no guarantee the security of the Member States is improved at all.

The risk and impact assessment as referred to in chapter 2 demonstrate that the vulnerability of the intra-European supply chains are large and that the consequences, both in term of fatalities and economic damage can be enormous.

Therefore the measures, proposed by this study to improve the security of the supply chain have the objective to prevent or reduce the consequences of all possible terrorist interventions in all supply chains within Europe, being it rail, road, inland waterways or short sea shipping.

It is recommended that the EC formulates a regulation containing detailed requirements to the European supply chain operators how to implement security management in their organisation, initially voluntary but in a few year time compulsory.

To ensure that parties in the supply chain operate on an equal level of security a system of initial and periodic audits by either newly to establish inspectorates, newly to nominate Recognised Security Organisations or accredited 3rd party certification bodies needs to be established.

Further, like with any regulation, there is no sustainability without enforcement. The Member States need to perform inspection, similar to the safety inspections they are presently performing on the transport sector. The capacity of the inspectorates performing these inspections now needs to be enlarged.

Implementation of such a regulation is only successful when all parties have sufficient awareness about the threat which terrorists impose on the EU and how implementing the regulation reduces this risk.

Detailed security requirements cannot be implemented when it has not been defined what seals, as used by industry will be accepted throughout Europe, and it is recommended that the industry develops smart ways to reduce the cost of employee vetting.

It is a fact that since 9/11 the number of terrorist atrocities in Europe has been showing an upward trend. Besides it needs to be accepted that terrorist interventions are a moving target. If
the authorities have found an adequate response to one type of terrorist acts the terrorist will move on to new types of attacks. It therefore needs to be accepted that measures to improve security, also those for the intra EU supply chains, are not to be seen as incidents but are measures which Europe has to live with for the years to come and which over time only may become tighter.

Making the supply chain more secure will not only reduce the chance on fatalities or serious damage to the European economy, it also will reduce the risk that European enterprises sustain serious losses or even are wiped out due to terrorist actions. Besides, given the complex nature supply chains may take, neither the Member States nor the industry are able to arrive at an acceptable level of security without each other. Therefore the public and private sectors need to cooperate since they are both responsible for and stakeholders in secure supply chains.

The study has proven that the level of awareness, the degree of maturity and the level of organisation regarding supply chain security with the respective traffic Member States shows large differences. Also the level of awareness in industry is evolving in a too slow pace.

This means that it easily may happen that individual Member States or enterprises may respond impulsively when a terrorist incident involving the supply chain occurs. Therefore, to avoid that un-harmonised solutions by individual Member States or companies disrupt the level playing field and will create undesired competitive effects for a single group of operators in the supply chain, the regulation should be launched quickly and there needs to be a systematic approach to the implementation of the regulation throughout the union.

Member states should implement the same requirements along the same implementation model and industry needs to include security as one of the quality aspects of their operation. They should take their responsibility for the security of their company and society at large and ensure that following secure procedures and applying security thinking becomes a normal part of daily life for all of those that are working in the supply chain. Only then the occurrence of undesired events is effectively prevented and companies will be able to quickly regain their normal operations when incidents happen.

At present the awareness of the need for security management is fairly low. It can only grow through an evolutionary process. Only when a real serious terrorist atrocity, directly related to the supply chain, occurs the awareness level will raise shock wise.

The Member States should ensure that reciprocity is maintained between them selves, but also between their transportation and their customs environments so the cost for implementation to industry is kept to a minimum.
7.2 Recommendations

For each of the developed frameworks, concerning the supply chain security requirements and the conditional and supportive instruments, recommendations have been formulated which need to be followed up in order to ensure correct implementation.

7.2.1 Supply Chain security management

1. The EC should develop supply chain security legislation which refers to the ISO PAS 28000 series as the minimum security standards which operators have to fulfil before they can be awarded the status of secure operator. The scope of the legislation covers:
   a. The whole supply chain
   b. All steps of the supply chain
   c. All transport modes
   d. All operators
2. The EC should develop the minimum security standards as a scheme in which operators in supply chain can initially participate on a voluntary basis to achieve a gradual implementation and development of supply chain security in the markets.
3. The EC should define the Supply Chain Manager approach as the preferred implementation approach.
4. The Member States should implement legislation which requires identification and registration of the Supply Chain Managers on the freight documents.
5. The Member States should be responsible for persuading Supply Chain Managers in implementing supply chain security in their supply chains. The Member States should assign an authority responsible for the coordination and supervision of the application of supply chain security by the Supply Chain Managers and their supply chain operators.
6. If persuaded to participate, the Supply Chain Managers should ensure that supply chain security management is implemented in its organisation and supply chains. It should be responsible for ensuring that all operators in their supply chain are secure operators.
7. Trade associations should provide supporting tools to micro companies to support implementation of security management in compliance with the requirements.
8. The EC should ensure that after the initial voluntary phase the requirements are enforced on all eligible operators from 2009.

Impact summary:

<table>
<thead>
<tr>
<th></th>
<th>Micro</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of companies</td>
<td>4.208.300</td>
<td>424.800</td>
<td>98.000</td>
<td>19.300</td>
<td>4.750.443</td>
</tr>
<tr>
<td>Share of the total freight flow*</td>
<td>6.0%</td>
<td>13.5%</td>
<td>20.7%</td>
<td>59.9%</td>
<td>100%</td>
</tr>
<tr>
<td>Companies affected by legislation**</td>
<td>4.171.245</td>
<td>391.300</td>
<td>58.906</td>
<td>4.568</td>
<td>4.626.019</td>
</tr>
<tr>
<td>Share of the freight flow affected</td>
<td>5.9%</td>
<td>12.4%</td>
<td>12.4%</td>
<td>14.2%</td>
<td>44.9%</td>
</tr>
<tr>
<td>Average implementation cost/company p.a. (x1000 euros)</td>
<td>5</td>
<td>50</td>
<td>135</td>
<td>300</td>
<td>-</td>
</tr>
<tr>
<td>Average maintenance cost/company p.a. (x1000 euros)</td>
<td>3</td>
<td>39</td>
<td>131</td>
<td>304</td>
<td>-</td>
</tr>
<tr>
<td>Total implementation costs (M€)</td>
<td>19.685</td>
<td>19.657</td>
<td>7.945</td>
<td>1.371</td>
<td>48.658</td>
</tr>
<tr>
<td>Total maintenance costs (M€)</td>
<td>11.709</td>
<td>15.416</td>
<td>7.704</td>
<td>1.389</td>
<td>36.218</td>
</tr>
</tbody>
</table>
### Annual costs for industry ***

<table>
<thead>
<tr>
<th>Year</th>
<th>Cost Calculation</th>
<th>Cost (M€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>( \frac{1}{4} \times 48.658 )</td>
<td>12.165</td>
</tr>
<tr>
<td>2007</td>
<td>( \frac{1}{4} \times 48.658 + \frac{1}{4} \times 36.218 )</td>
<td>21.220</td>
</tr>
<tr>
<td>2008</td>
<td>( \frac{1}{4} \times 48.658 + \frac{1}{2} \times 36.218 )</td>
<td>30.274</td>
</tr>
<tr>
<td>2009</td>
<td>( \frac{1}{4} \times 48.658 + \frac{3}{4} \times 36.218 )</td>
<td>39.329</td>
</tr>
<tr>
<td>Onward</td>
<td>36.218 M€ annually</td>
<td></td>
</tr>
</tbody>
</table>

### Benefits for industry

- Increased sustainability and resilience of organisations
- Commercial advantage for service providers
- Reduced number of cargo inspections
- Reduction of cargo theft
- Reduced chance on brand- and reputation damage
- Increased efficiency and transparency
- Common minimum security standards results in level playing field

### Benefits for the Member states

- Reduced risk of fatalities
- Reduced risk of economic damage
- One common approach throughout EU and across transport modes
- Equal confidence in security of different modes and Member States.

### Possible negative security effect

- If the same security level is not achieved in the whole supply chain, then in spite of all investments, little has been achieved. Supply chain security is as strong as its weakest link.
- Implementation of security measures creates a sense of security which may result in reduced awareness (to suspicious activities).
- Incorrect implementation of supply chain security may create a false sense of security. Security control inspections are reduced even though the supply chain is not secure.
- However, even correct implementation of supply chain security can create a false sense of security. 100% security cannot be achieved.

*) Based on the relative production value of the manufacturers in each size category

**) Approximately 125,000 companies are not included in the cost assessment. They are assumed to be already participating in other EU and US customs security requirements. Through the proposed principle of mutual recognition compliance to these other security requirements also ensures compliance to the supply chain security requirements.

***) During the voluntary roll out, 2006-2009, a linear participation curve is assumed. This means each year a quarter of all companies decides to comply with the requirements. After the voluntary roll out, when the program becomes mandatory, all implementation costs will have been made and only the annual costs remain.

### 7.2.2 Audit scheme

1. The EC must develop legislation for the establishment of mandatory audit program by Member States which audits operators’ compliance to the EU supply chain security requirements and awards a secure operator label to those operators which fulfil those requirements.

2. The legislation must include:
   a. The award criteria on which the secure operator status is awarded.
   b. Registration procedures for secure operators.
   c. Mutual recognition clause.

3. The EC should develop auditing criteria in line with accreditation practices to which the auditing organisations and staff must comply, to ensure harmonised auditing of supply chain operators and allow mutual recognition of secure operator labels.

4. Member states should set up national supply chain security audit programs and decide whether to use national inspectorates, Recognised Security Organisations or certification bodies to perform the security management audits.
5. The supply chain managers and operators are responsible for their organisations to be audited by their national auditing body.

Impact summary:

| Share of companies affected by audit scheme* | Gradually growing to 4.626.019 |
| Number of auditors involved | Growing to 7000 |
| Cost for all Member States combined ** | 2.700 M€ |
| Cost for per Member States (average) | € 5.92 per inhabitant |

| Cost for Industry** | Only when Member States decide to delegate auditing to third parties will costs have to be borne by industry. These will be of same order as for Member States (see remark below) |
| Annual audit costs *** | 2006 | ¼ * 2.700 = 675 M€ |
| | 2007 | ¼ * 2.700 + ¼ * 1.167 = 967 M€ |
| | 2008 | ¼ * 2.700 + ½ * 1.167 = 1.259 M€ |
| | 2009 | ¼ * 2.700 + ¾ * 1.167 = 1.550 M€ |
| Onwards | 1.167 M€ annually |

Benefits to the Member states

- Ensuring the implementation and maintenance of the security management systems and mitigation measures.
- Creation of a secure operator label by which supply chains and operators who have successfully implemented the minimum requirements can be recognised.
- Security control measures can be focused on operators not part of secure supply chains.
- Mutual recognised security label supports a common security approach which increases predictability.
- Interconnectivity with the Known Consignor and the Authorised Economic Operator concepts in the aviation and customs sectors.

Benefits to industry

- Common EU audit scheme results in level playing field for industry.
- Common EU audit scheme allows mutual recognition and thus prevents multiple auditing.
- Secure operator label allows participating organisations to enjoy green lane treatment.
- Secure operator label allows participating organisations to positively distinguish themselves.

Possible negative security effect

- If audits are not of the same quality level throughout the EU, not only will the level playing field be disturbed, the security level also cannot be guaranteed. Creating a false sense of security.

*) Costs are calculated for when Member states decide to establish National Inspectorates. If Member States decide to delegate auditing to Recognised Security Organisations or 3rd party Certification bodies these cost will be absorbed by industry. The cost for industry will be of the same order as calculated for the Member States.

**) During the voluntary roll out, 2006-2009, a linear participation curve is assumed. This means each year a quarter of all companies decides to comply with the requirements. After the voluntary roll out, when the program becomes mandatory, all implementation costs will have been made and only the annual costs remain.

7.2.3 Enforcement scheme

1. The EC must develop legislation for the establishment of mandatory enforcement program by Member States which inspects and monitors operators’ compliance to the EU supply chain security requirements. The legislation must include:
a. The requirement that Member States setup inspectorates to inspect EU supply chain security conformity.
b. The requirement that Member States develop “green lanes” to provide facilitations to proved secure operators.
c. The rules for suspension or withdrawal of the “green lane” status.
d. A common structure for fines to ensure that non-conformities in the mandatory phase result in similar fines in all Member States.

2. EC facilitates the development of a common inspection database where data of certified secure operators is stored to support data exchange between the Member State inspectorates.

3. Member States should assign security inspection activities and responsibilities to national inspectorates / authorities. Where possible existing inspectorates such as traffic inspectorates and labour/work safety inspectorates are used. Resource allocations are arranged accordingly.

4. Security inspectorates should set up and implement national inspection programs and develop “green lane” programs for proved secure operators.

**Impact summary:**

<table>
<thead>
<tr>
<th></th>
<th>2006-2009 (voluntary roll out phase)</th>
<th>Onward (mandatory phase)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of EU-freight flow</td>
<td>Gradually growing to spot checks on 10%</td>
<td>0-5%</td>
</tr>
<tr>
<td>Required inspection staff</td>
<td>7000</td>
<td>2000</td>
</tr>
<tr>
<td>Cost for the Member States combined</td>
<td>450 M€ p.a.</td>
<td>50 M€ p.a.</td>
</tr>
<tr>
<td>Cost for the Member States (average)</td>
<td>€ 1,00 per inhabitant p.a.</td>
<td>€ 0,10 per inhabitant p.a.</td>
</tr>
</tbody>
</table>

**Benefits to the Member states**
- Verify continued implementation and effectiveness of security management systems and mitigation measures.
- Resolves incorrect implementation / application of measures which may damage the effectiveness of the measures.
- Safety net under the periodic audits

**Possible negative security effect**
- None identified

### 7.2.4 Awareness programs

1. The EC should define the minimum requirements the national and industry awareness campaigns must meet and also define a format within which the campaigns can be developed.

2. The EU should develop a mould for promotional and communication materials for the EU Member States.

3. National authorities and trade associations should develop, with support of the EU their national or sector security awareness programs and are provided with EU promotional and information materials.

4. The industry should implement the developed awareness campaigns under the leadership of the industrial leaders.

5. Operators should setup bottom up security information channels.
Impact summary:

<table>
<thead>
<tr>
<th>From 2006 onwards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of EU-freight flow</td>
</tr>
<tr>
<td>Cost for the Member States</td>
</tr>
<tr>
<td>Costs for industry</td>
</tr>
<tr>
<td>Cost for the EC</td>
</tr>
<tr>
<td>Benefits to the Member states</td>
</tr>
<tr>
<td>Benefits to industry</td>
</tr>
<tr>
<td>Possible negative security effect</td>
</tr>
</tbody>
</table>

7.2.5 Employee vetting system

1. EC should develop EU vetting requirements which include:
   a. What aspects of the employee’s background need to be checked.
   b. The grounds on which the employee is declared secure or un-secure.
2. Member States together with trade and labour industries should develop a vetting programme which meets both national privacy legislation as well as the EU vetting requirements. The developed program should be verified by the EC on its compliance to the EU requirements.
3. Operators should accept vetting results from EU compliant vetting programmes.

Impact summary:

<table>
<thead>
<tr>
<th>From 2006 onwards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of EU-freight flow</td>
</tr>
<tr>
<td>Cost for the Member States</td>
</tr>
<tr>
<td>Cost for industry</td>
</tr>
<tr>
<td>Benefits to Industry</td>
</tr>
<tr>
<td>Possible negative security effect</td>
</tr>
</tbody>
</table>
7.2.6 Seal programme

1. The EC should develop a standard for seals and seal programs based on the existing WCO seal program.
2. The standard should become part of the EU supply chain security requirements.
3. Supply chain operators implementing security management in their organisations to comply with the EU supply chain security requirements should ensure that the implemented seal program should comply with the EU seal and seal program standard.

Impact summary:

<table>
<thead>
<tr>
<th>Impact summary:</th>
<th>From 2006 onwards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of EU-freight flow</td>
<td>Growing to 100%</td>
</tr>
<tr>
<td>Cost for the Member States</td>
<td>None</td>
</tr>
<tr>
<td>Cost for the EU</td>
<td>Minor costs are necessary to translate the standard to legislation</td>
</tr>
<tr>
<td>Cost for industry</td>
<td>None</td>
</tr>
<tr>
<td>Application of seals are part of the drafted security requirements for which the costs have been calculated in 7.1. There are no financial implications caused by the seal standardisation programme. Its only intention is to allow better compatibility.</td>
<td></td>
</tr>
<tr>
<td>Benefits to Member States</td>
<td>• Is conditional for verification if security has been violated en route</td>
</tr>
<tr>
<td>Possible negative security effect</td>
<td>• If the applied seals are not of the right quality and do not meet the technical specifications, there will be a possibility of fraud. The cargo may look secure but is all but secure and thus creates a false sense of security.</td>
</tr>
</tbody>
</table>
is a different kind of consulting firm, offering advanced cross-disciplinary competence within management and technology. Our consulting approach reflects the new risk agenda in high-risk and capital-intensive industries. We have a firm base in DNV's strong technological competencies, international experience and unique independence as a foundation. Our consultants serve international clients from locations in Norway, UK, Germany, Benelux and the USA.
Summary Appendix I: Detailed supply chain security requirements
### Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport Inland</th>
<th>Waterway</th>
<th>Ware-housing Forward etc</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records (Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

#### General system requirements

- Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons
- Ensure that security critical staff including sub-contracted staff are screened and interviewed prior to employment and reasonable intervals.
- All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training

#### Human Resource Security

- Implement procedures how deviations and anomalies are handled
- Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled,
- Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies
- Ensure that random, unannounced security verification of areas in control of the organisation and within the supply chain are performed.
- Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.
- Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills
- Ensure inspection of confined spaces of the means of transport before (re)delivery
- Ensure adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions.
- Ensure that a trusted employee is physically present during loading/unloading of the cargo unit to supervise the introduction or removal of cargo to prevent that the physical security of the cargo is inflicted. This supervision shall be uninterrupted from the start of the inspection until the cargo is sealed
## Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forward agents etc</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that this trusted employee at closing of the cargo unit is providing it with a seal and record relevant details in compliance with the companies sealing procedure</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure verification that seals on received cargo are intact and conform the appropriate records.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that empty or partially loaded cargo units are inspected to detect any security breach or compromising of the integrity of the unit immediately before loading</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all cargo is compliant with its documentation and manifests</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that any units partly packed at end of business are securely locked to restrict access.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that origin site pre-alerts destination site before shipment. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that seals are stored under controlled conditions, not be used in numeric sequence and that records on seals are verified by a second person</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only containers, swap bodies, trailers etc are used which are acceptable to the regulatory authorities.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check that all cargo entering the premises are properly sealed and that the seal or alternative access monitoring devices and where possible the cargo is compliant to its documentation</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading and check pre-alert information from origin site. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that emptied cargo units are sealed again, with proper recording of such seals, or otherwise are secured against unauthorised access.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only cargo is accepted to be loaded on the organisations means of conveyance which are properly marked, have the correct weight and documentation, and that the marking of the cargo (unit) and its seals are in accordance with the documentation.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that cargo units, whether stuffed-up or empty, only will be loaded when they are properly sealed and this sealing is properly recorded.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that cargo is moved according to pre-defined schedules, including routes and stops, and unexpected delays and deviations are reported to the organisation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forwarding</th>
<th>Agents etc</th>
<th>Shippers</th>
<th>Manufacturers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that before loading, at departure and after each prolonged stop seals are checked for tampering, all readily accessible areas are physical searched and internal/external compartments and panels and other potential places of concealment of illegal or illicit goods are secured and/or inspected. These checks are to be recorded and records are to be kept for three months and be accessible to other actors in the supply chain for verification.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure rerouting of dangerous cargo to avoid routine patterns</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that no unauthorised passengers are allowed on board.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that confined spaces are inspected after delivery or at redelivery after maintenance or repair.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that vessels and barges are kept under constant surveillance, whether en route or boarded alongside and have adequate lightening to prevent intrusion</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that control rooms of traffic control centres are kept locked for non-authorised persons.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that an analysis is made of the vulnerability of information systems, the relevance to security of data and the implementation of adequate safeguards and firewalls.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that files and records are not removed from the office without permission.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all computer users acknowledge receipt of, and consent to, the IT security policy as a condition of access to company systems.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all IT personnel with access to digital information, including those with indirect access by means of administrative privilege, receive training on information security principles. For certain personnel, this may include training on proper incident handling procedures.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that complete, legible and accurate documents, either electronically or conventionally, are submitted timely to designated authorities, in the format, means and at the time requested by them.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that security critical information is securely stored, only accessible to authorised personnel and that the users of this information can be traced back</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the security officer regularly checks information access logs to identify any unusual or out-of-hours activity.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that routines exist to securely cope with break downs and secure back-up routines are followed.</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that the transporter or cargo owner is informed when during the processing of information it is noted that the progress or movement of cargo deviates from pre-defined schedules</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that overages and shortages, as well as other anomalies, observed during the processing of information, are reported not only to the designated authorities, but also to the organisation(s) responsible for the processing of the cargo.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland</th>
<th>Waterway</th>
<th>Ware-housing</th>
<th>Forward agents etc</th>
<th>Shippers</th>
<th>Manufact.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure buildings containing critical working areas are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorised persons and goods.</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, situated outside, are surrounded by perimeter fences which comply to the legal and statutory requirements</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas are fitted with doors, windows, gates and fences, provided with adequate locking devices.</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, both inside and outside, as well as parking areas are provided with adequate lighting</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas are equipped with intrusion alarms or its equivalent and that alarms are subject to 24 hour response and real time monitoring</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that parking areas for private vehicles are well separated from critical working areas</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that critical working areas, where appropriate, are patrolled by guards, dogs and/or closed TV-circuits.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that all loading and discharge valves and inspection hatches of dangerous cargo transports are provided with (pad)locks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that dry-bulk cargo is covered by tarpaulins or hatches, which are properly sealed.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that international-, domestic-, high-value- and dangerous goods cargo is marked and segregated within the premises by a safe, caged or otherwise fenced-in area.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that dangerous goods are kept segregated from other cargo.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that control cabins of means of conveyance, when not manned, are kept locked at all times and only employees of the organisation are allowed to have access.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that keys are kept under control of the driver/operator at all times.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that documentation containing cargo information is kept secure in these control cabins.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that control cabins are equipped with an intrusion alarm.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that other internal or external compartments or panels are kept locked when not under surveillance.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that procedures are in place for reporting when unauthorised persons, un-manifested materials, or signs of tampering, are discovered.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that no prolonged stops are made at isolated locations where normal social control can not be exercised, unless such location is equipped with adequate lightening (and fencing) according to the standards set by the designated authorities.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements

**DESCRIPTION OF REQUIREMENT**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rail repair shops</th>
<th>Road transport</th>
<th>Rail Transport</th>
<th>Inland Waterway</th>
<th>Warehousing</th>
<th>Forwarding</th>
<th>Agents etc</th>
<th>Shippers</th>
<th>Manufactur</th>
<th>Engage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that only authorised staff has access to critical working areas.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controls shall include positive identification and recording of all arriving and leaving employees, suppliers, visitors, vendors and incoming vehicles and their drivers.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that visitors are not moving around the facilities without</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accompaniment of a trusted employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that unauthorised / unidentified persons are stopped and questioned</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that restricted areas are clearly marked as such and unauthorised access to these areas is prevented or raises an alarm.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that authorisation to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorised persons for which records shall be held.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organisation for which records shall be held.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Auditing**

- The organisation shall plan internal audits and follow-up possible improvements needed. | X | X | X | X | X | X | X | X | X | X | X |
- The organisation shall be audited by an authorised external party to ensure compliance to above requirements | X | X | X | X | X | X | X | X | X | X | X |
Summary Appendix II: ISO PAS 28000 Series
DRAFT PUBLICLY AVAILABLE SPECIFICATION
ISO/CD/PAS 28000

SPECIFICATION FOR SECURITY MANAGEMENT SYSTEMS
FOR THE SUPPLY CHAIN
Contents

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Security management system elements
   4.1 General requirements
   4.2 Security management policy
   4.3 Security risk assessment and planning
   4.4 Implementation and operation
   4.5 Checking and corrective action
   4.6 Management review and continual improvement
Annex A Bibliography
Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on the committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 28000 was prepared by Technical Committee ISO/TC 8, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.
Introduction

This Publicly Available Specification has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. This Specification is a high level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1.
This Specification is intended to apply in cases where an organization’s supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with a Specification does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system to this Specification may be verified by an external or internal auditing process.

This Specification is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this Specification. It is not the intention of this specification to duplicate...
governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

Note: This specification is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows:

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization’s security policy
- Do: implement the processes
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results
- Act: take actions to continually improve performance of the security management system

1. **Scope**

This Specification specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This Specification is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) establish, implement, maintain and improve a security management system;
b) assure compliance with stated security management policy;
b) assure compliance with stated security management policy;
c) demonstrate such compliance to others;
c) demonstrate such compliance to others;
d) seek certification/registration of its security management system by an Accredited
d) seek certification/registration of its security management system by an Accredited third party Certification Body; or
third party Certification Body; or
e) make a self-determination and self-declaration of compliance with this
e) make a self-determination and self-declaration of compliance with this Specification.
Specification.

There are legislative and regulatory codes that address some of the requirements in this specification. It is not the intention of this standard to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

2. Normative references

None

3. Terms and Definitions

For the purposes of this specification, the following terms and definitions apply:

3.1 Facility(ies): plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service.

NOTE: This definition includes any software code that is critical to the delivery of security and the application of security management.
3.2 Security: resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.

3.3 Security management: systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from.

3.4 Security management objective: specific outcome or achievement required of security in order to meet the security management policy.

NOTE: It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.5 Security management policy: overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization’s policy and regulatory requirements.

3.6 Security management programmes: the means by which a security management objective is achieved.

3.7 Security management target: specific level of performance required to achieve a security management objective.

3.8 Stakeholder: person or entity having a vested interest in the organization’s performance, success or the impact of its activities.

NOTE: Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations, or society.
3.9 Supply chain: the linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

3.9.1 Downstream: refers to the actions, processes and movements of the cargo in the supply chain that occur after the cargo leaves the direct operational control of the organization, including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.

3.9.2 Upstream: refers to the actions, processes and movements of the cargo in the supply chain that occur before the cargo comes under the direct operational control of the organization. Including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.

3.10 Top Management: person or group of people who directs and controls an organization at the highest level.

NOTE: Top management, especially in a large multinational organization, may not be personally involved as described in the Specification; however top management accountability through the chain of command shall be manifest.

3.11 Continual Improvement: recurring process of enhancing the security management system in order to achieve improvements in overall security performance consistent with the organization’s security policy.

4. Security management system elements
4.1 General requirements

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security risks and controlling and mitigating their consequences.

The organization shall continually improve its effectiveness in accordance with the requirements set out in the whole of Clause 4.

The organization shall define the scope of its security management system. Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such processes are controlled. The
necessary controls and responsibilities of such outsourced processes shall be identified within the security management system.

4.2 Security management policy

The organization’s top management shall authorize an overall security management policy. The policy shall:

a) be consistent with other organizational policies;
b) provide the framework which, enables the specific security management objectives, targets and programmes to be produced;
c) be consistent with the organization’s overall security threat and risk management framework;
d) be appropriate to the threats to the organization and the nature and scale of its operations;
e) clearly state the overall/broad security management objectives;
f) include a commitment to continual improvement of the security management process;
g) include a commitment to comply with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes;
h) be visibly endorsed by top management;
i) be documented, implemented and maintained;
j) be communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security management-related obligations;
k) be available to stakeholders where appropriate;
l) provide for its review in case of the acquisition of, or merger with other organizations, or other change to the business scope of the organization which may affect the continuity or relevance of the security management system.
NOTE: Organizations may choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which may be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its stakeholders and other interested parties.

4.3 Security risk assessment and planning

4.3.1 Security risk assessment

The organization shall establish and maintain procedures for the ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures. Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences which shall include:

a) physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;

b) operational threats and risks, including the control of the security, human factors and other activities which affect the organization’s performance, condition or safety;

c) natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;

d) factors outside of the organization’s control, such as failures in externally supplied equipment and services;

e) stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;

f) design and installation of security equipment including replacement, maintenance, etc.

g) information and data management and communications.

h) a threat to continuity of operations
The organization shall ensure that the results of these assessments and the effects of these controls are considered and, where appropriate, provide input into:

a) security management objectives and targets;
b) security management programmes;
c) the determination of requirements for the design, specification and installation;
d) identification of adequate resources including staffing levels;
e) identification of training needs and skills (see 4.4.2);
f) development of operational controls (see 4.4.6);
g) the organization’s overall threat and risk management framework.

The organization shall document and keep the above information up to date.

The organization’s methodology for threat and risk identification and assessment shall:

a) be defined with respect to its scope, nature and timing to ensure it is proactive rather than reactive;
b) include the collection of information related to security threats and risks;
c) provide for the classification of threats and risks and identification of those that are to be avoided, eliminated or controlled;
d) provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (see 4.5.1).

4.3.2 Legal, statutory and other security regulatory requirements

The organization shall establish, implement and maintain a procedure

a) to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and
b) to determine how these requirements apply to its security threats and risks.
The organization shall keep this information up-to-date. It shall communicate relevant information on legal and other requirements to its employees and other relevant third parties including contractors.

4.3.3 Security management objectives

The organization shall establish, implement and maintain documented security management objectives at relevant functions and levels within the organization. The objectives shall be derived from and consistent with the policy. When establishing and reviewing its objectives, an organization shall take into account:

a) legal, statutory and other security regulatory requirements;
b) security related threats and risks;
c) technological and other options;
d) financial, operational and business requirements;
e) views of appropriate stakeholders.

The security management objectives shall be:

a) consistent with the organization’s commitment to continual improvement;
b) quantified (where practicable);
c) communicated to all relevant employees and third parties, including contractors, with the intent that these persons are made aware of their individual obligations;
d) reviewed periodically to ensure that they remain relevant and consistent with the security management policy. Where necessary the security management objectives shall be amended accordingly.

4.3.4 Security management targets

The organization shall establish, implement and maintain documented security management targets appropriate to the needs of the organization. The targets shall be derived from and be consistent with the security management objectives.
These targets shall be:

a) to an appropriate level of detail;
b) specific, measurable, achievable, relevant and time-based (where practicable);
c) communicated to all relevant employees and third parties including contractors with the intent that these persons are made aware of their individual obligations;
d) reviewed periodically to ensure that they remain relevant and consistent with the security management objectives. Where necessary the targets shall be amended accordingly.

4.3.5 Security management programmes

The organization shall establish, implement and maintain security management programmes for achieving its objectives and targets.

The programmes shall be optimized and then prioritized, and the organization shall provide for the efficient and cost effective implementation of these programmes.

This shall include documentation which describes:

a) the designated responsibility and authority for achieving security management objectives and targets;
b) the means and time-scale by which security management objectives and targets are to be achieved.

The security management programmes shall be reviewed periodically to ensure that they remain effective and consistent with the objectives and targets. Where necessary the programmes shall be amended accordingly.

4.4 Implementation and operation

4.4.1 Structure, authority and responsibilities for security management
The organization shall establish and maintain an organizational structure of roles, responsibilities and authorities, consistent with the achievement of its security management policy, objectives, targets and programmes. These roles, responsibilities and authorities shall be defined, documented and communicated to the individuals responsible for implementation and maintenance. Top management shall provide evidence of its commitment to the development and implementation of the security management system (processes) and continually improving its effectiveness by:

   a) appointing a member of top management who, irrespective of other responsibilities, shall be responsible for the overall design, maintenance, documentation and improvement of the organization’s security management system;

   b) appointing (a) member(s) of management with the necessary authority to ensure that the objectives and targets are implemented;

   c) identifying and monitoring the requirements and expectations of the organization’s stakeholders and taking appropriate and timely action to manage these expectations;

   d) ensuring the availability of adequate resources;

   e) considering the adverse impact that the security management policy; objectives, targets, programmes, etc. may have on other aspects of the organization;

   f) ensuring any security programmes generated from other parts of the organization complement the security management system;

   g) communicating to the organization the importance of meeting its security management requirements in order to comply with its policy;

   h) ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate;

   i) ensuring the viability of the security management objectives, targets and programmes.

### 4.4.2 Competence, training and awareness
The organization shall ensure that personnel responsible for the design, operation and management of security equipment and processes are suitably qualified in terms of education, training and/or experience. The organization shall establish and maintain procedures to make persons working for it or on its behalf aware of:

a) the importance of compliance with the security management policy and procedures, and to the requirements of the security management system;

b) their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements;

c) the potential consequences to the organization’s security by departing from specified operating procedures.

Records of competence and training shall be kept.

4.4.3 Communication
The organization shall have procedures for ensuring that pertinent security management information is communicated to and from relevant employees, contractors and other stakeholders.

Because of the sensitive nature of certain security related information, due consideration should be given to the sensitivity of information prior to dissemination.

4.4.4 Documentation
The organization shall establish and maintain a security management documentation system that includes, but is not limited to the following:

a) the security policy, objectives and targets

b) description of the scope of the security management system,

c) description of the main elements of the security management system and their interaction, and reference to related documents,

d) documents, including records, required by this International Standard, and
e) determined by the organization to be necessary to ensure the effective planning, 
operation and control of processes that relate to its significant security threats and risks.

The organization shall determine the security sensitivity of information and shall take steps to prevent unauthorized access.

4.4.5 Document and data control

The organization shall establish and maintain procedures for controlling all documents, data and information required by Clause 4 of this Specification to ensure that:

a) these documents, data and information can be located and accessed only by authorized individuals;

b) these documents, data and information are periodically reviewed, revised as necessary, and approved for adequacy by authorized personnel;

c) current versions of relevant documents, data and information are available at all locations where operations essential to the effective functioning of the security management system are performed;

d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;

e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified;

f) these documents, data and information are secure, and if in electronic form are adequately backed up and can be recovered.

4.4.6 Operational control

The organization shall identify those operations and activities that are necessary for achieving:

a) its security management policy;

b) the control of identified security threats and risks;

c) compliance with legal, statutory and other regulatory security requirements;
d) its security management objectives;
e) the delivery of its security management programmes;
f) the required level of supply chain security.

The organization shall ensure these operations and activities are carried out under specified conditions by:

a) establishing, implementing and maintaining documented procedures to control situations where their absence could lead to failure to achieve the operations and activities listed in 4.4.6 a) to f) above;
b) evaluating any threats posed from upstream supply chain activities and applying controls to mitigate these impacts to the organization and other downstream supply chain operators;
c) establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors.

These procedures shall include controls for the design, installation, operation, refurbishment, and modification of security related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced, that could impact on security management operations and activities, the organization shall consider the associated security threats and risks before their implementation. The new or revised arrangements to be considered shall include:

a) revised organizational structure, roles or responsibilities;
b) revised security management policy, objectives, targets or programmes;
c) revised processes and procedures;
d) the introduction of new infrastructure, security equipment or technology, which may include hardware and/or software;
e) the introduction of new contractors, suppliers or personnel, as appropriate.

4.4.7 Emergency preparedness, response and security recovery
The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them. The plans and procedures shall include information on the provision and maintenance of any identified equipment, facilities or services that can be required during or after incidents or emergency situations.

The organization shall periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats. The organization shall periodically test these procedures where practicable.

4.5 Checking and corrective action

4.5.1 Security performance measurement and monitoring

The organization shall establish and maintain procedures to monitor and measure the performance of its security management system. It shall also establish and maintain procedures to monitor and measure the security performance. The organization shall consider the associated security threats and risks, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance parameters. These procedures shall provide for:

a) both qualitative and quantitative measurements, appropriate to the needs of the organization;

b) monitoring the extent to which the organization’s security management policy, objectives and targets are met;

c) proactive measures of performance that monitor compliance with the security management programs, operational control criteria and applicable legislation, statutory, and other security regulatory requirements;

d) reactive measures of performance to monitor security-related deteriorations, failures, incidents, non-conformances (including near misses and false alarms) and other historical evidence of deficient security management system performance;
e) recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventative action analysis. If monitoring equipment is required for performance and/or measurement and monitoring, the organization shall require the establishment and maintenance of procedures for the calibration and maintenance of such equipment. Records of calibration and maintenance activities and results shall be retained for sufficient time to comply with legislation and the organization’s policy.

4.5.2 System evaluation

The organization shall evaluate security management plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors must be reflected immediately in the procedure(s).

The organization shall periodically evaluate compliance with relevant legislation and regulations, industry best practices, and conformance with its own policy and objectives.

The organization shall keep records of the results of the periodic evaluations.

4.5.3 Security-related failures, incidents, non-conformances and corrective and preventive action

The organization shall establish, implement and maintain procedures for defining responsibility and authority for:

a) evaluating and initiating preventive actions to identify potential failures of security in order that that may be prevented from occurring;

b) the investigation of security-related:
   i) failures including near misses and false alarms;
ii) incidents and emergency situations;

iii) non-conformances;

c) taking action to mitigate any consequences arising from such failures, incidents or non-conformances;

d) the initiation and completion of corrective actions;

e) the confirmation of the effectiveness of corrective actions taken.

These procedures shall require that all proposed corrective and preventive actions are reviewed through the security threat and risk assessment process prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety.

Any corrective or preventive action taken to eliminate the causes of actual and potential non-conformances shall be appropriate to the magnitude of the problems and commensurate with the security management-related threats and risks likely to be encountered. The organization shall implement and record any changes in the documented procedures resulting from corrective and preventive action and shall include the required training where necessary.

4.5.4 Control of Records

The organization shall establish and maintain records as necessary to demonstrate conformity to the requirements of its security management system and of this standard, and the results achieved.

The organization shall establish, implement and maintain a procedure(s) for the identification, storage, protection, retrieval, retention and disposal of records.

Records shall be and remain legible, identifiable and traceable.

Electronic and digital documentation should be rendered tamper proof, securely backed-up and accessible only to authorized personal.
4.5.5 Audit

The organization shall establish, implement and maintain a security management audit program and shall insure that audits of the security management system are carried out at planned intervals, in order to:

a) determine whether or not the security management system:
   i) conforms to planned arrangements for security management including the requirements of the whole of Clause 4 of this specification;
   ii) has been properly implemented and maintained;
   iii) is (are) effective in meeting the organization’s security management policy and objectives;

b) review the results of previous audits and the actions taken to rectify non-conformances;

c) provide information on the results of audits to management;

d) verify that the security equipment and personnel are appropriately deployed.

The audit program, including any schedule, shall be based on the results of threat and risk assessments of the organization’s activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results. Where possible, audits shall be conducted by personnel independent of those having direct responsibility for the activity being examined.

NOTE: The phrase “personnel independent” does not necessarily mean personnel external to the organization.

4.6 Management review and continual improvement

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.
Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the security policy and security objectives and threats and risks. Records of the management reviews shall be retained. Input to management reviews shall include

a) results of audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes,

b) communication(s) from external interested parties, including complaints,

c) the security performance of the organization,

d) the extent to which objectives and targets have been met,

e) status of corrective and preventive actions,

f) follow-up actions from previous management reviews,

g) changing circumstances, including developments in legal and other requirements related to its security aspects, and

h) recommendations for improvement.

The outputs from management reviews shall include any decisions and actions related to possible changes to security policy, objectives, targets and other elements of the security management system, consistent with the commitment to continual improvement.
Annex A

Bibliography

1  ISO 9001:2000
2  ISO 14001:2004
3  ISO 19011:2002
Report Appendix A: Infrastructure security assessment report template
Generic Infrastructure Element
Security Assessment Report Template

for

(Details of Location)

(Note this document is a specimen template intended to demonstrate a methodology. It should not be construed as being complete nor conformant to any regulation)

Prepared By
(Details of Author and Organisation)


When using this template each page shall be clearly marked with the wording **Confidential**

<table>
<thead>
<tr>
<th>Document No/Revision</th>
<th>Description</th>
<th>Prepared By:</th>
<th>Approved By:</th>
<th>This Version is based on Security Assessment:</th>
</tr>
</thead>
</table>

**Contents**

Section 1: Introduction .............................................................................................................. 3

Section 2: Threat Assessment .................................................................................................... 4

Section 3: Facility Management and Co-ordination .................................................................... 4

Section 4: Operational Overview ............................................................................................... 4

Section 5: Vulnerabilities .......................................................................................................... 5

Section 6: Counter Measures ..................................................................................................... 5

Section 7: Recommendations ..................................................................................................... 5

Section 8: Conclusions .............................................................................................................. 5
Section 1: Introduction

A Facility Assessment is a critical part of the process in producing a credible Security Plan.

The (Insert details, tunnel, bridge etc) covered by this assessment is located at (Insert details of location)

The Security Assessment included a full survey of the facility and supporting infrastructure. In accordance with best practice the following areas were addressed:

- The identification and evaluation of critical assets and infrastructure that it is important to protect
- The identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures
- The identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and
- The identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

This assessment report outlines the findings of the assessment and describes the measures and procedures that should be put into place with regard to the (Name of facility) The details contained within this survey report along with the existing security plans and procedures will form the basis of the Security Plan.
Section 2: Threat Assessment

(Insert relevant threat information for this infrastructure element).

(Insert an overview of any security procedures currently in place at this facility)

These procedures were reviewed and will be used along with the survey results to form the basis of the Security Plan.

A Risk / Threat analysis was conducted and the following areas were addressed:

(Insert a complete list of specific, identified threats)

The summary of the threat assessment is contained at Annex A to this report.

Section 3: Facility Management and Co-ordination

The (Insert name of facility) is located in the (Insert location details) and is managed by (Insert details of operational management).

(Insert description of facility)

(Insert description of management structure)

(Insert an overview of the security regime that is currently in place)

Section 4: Operational Overview

(Insert an Operational Overview covering:

Details of management structure

Type of traffic handled and volumes

Access Controls

The management of the staff and visitor pass systems

Details of the perimeter protection, patrols, search regimes etc.)
Section 5: Vulnerabilities

(Insert details of all vulnerabilities identified as a result of
1. The Vulnerability Assessment; and
2. The identified threats in Section Two)

Items could include:
Surveillance
Access Control
Restricted Areas
Checking of Vehicles/Vessels
Delivery of Stores and Materials
Monitoring of Security

Section 6: Counter Measures

(Give an overview of the counter measures currently in place at the facility and its surrounding infrastructure)

(Comment on the results of the Vulnerability Assessment highlighting any critical deficiencies)

Section 7: Recommendations

(Insert all recommendations that are required to bring the facility and its associated infrastructure up to an acceptable standard)

Section 8: Conclusions

(Insert concluding remarks including a brief appraisal of the facility and any particular problems encountered. Any extra information that may be useful for the compilation of the Security Plan should be included here)
Report Appendix B: Generic infrastructure security plan template
Generic Infrastructure Element
Security Plan Template

for

(Details of Location)

(Note this document is a specimen template intended to demonstrate a methodology. It should not be construed as being complete nor conformant to any regulation)

Prepared By
(Details of Author and Organisation)
When using this template each page shall be clearly marked with the wording

Confidential

<table>
<thead>
<tr>
<th>Document No/Revision</th>
<th>Description</th>
<th>Prepared By:</th>
<th>Approved By:</th>
<th>This Version is based on Security Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Infrastructure Security Plan</td>
<td></td>
<td></td>
<td></td>
<td>dd/mmm/yyyy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The contents of this document are strictly confidential and should not be disclosed to unauthorised personnel
Contents

Document Status and Revision Control ................................................................. 6

Purpose and Background ..................................................................................... 6
Definitions, Expressions and Abbreviations ...................................................... 7

Section 1: Infrastructure Details ......................................................................... 7

Section 2: Protection of Security Related Information ....................................... 10

2.1 Classification and Protection of the Security Plan ...................................... 10
2.2 Access to the Security Plan .......................................................................... 10
2.3 Safeguarding of Security Related Information ........................................... 10
2.4 Safeguarding Electronic Information ............................................................ 11

Section 3: Internal/External Audit, Review and Updating of the Security Plan ..... 12

3.1 Internal Audit ................................................................................................. 12
3.2 External Audit ................................................................................................. 12
3.3 Review and Updating of the Security Plan .................................................... 12
3.4 Approval of Updates ....................................................................................... 12
3.5 Reporting of Security Incidents or Breaches of Security ............................ 12

Section 4: Management of Security .................................................................... 14

4.1 Responsibility for Transport Infrastructure Security ..................................... 14
4.2 Details of security contractors (if used) and their contracted duties: .......... 15
4.3 Security Level Changes .................................................................................. 16
4.4 Security Organisation Chart ......................................................................... 17
4.5 Response to and Reporting of Security Threats, Incidents and Breaches of Security .............................................................................................................. 17
4.6 Security Equipment ......................................................................................... 18

Section 5: Interface with Relevant Agencies ...................................................... 19

5.1 Exchange of Information .............................................................................. 19
5.2 Coordination of Security Measures .............................................................. 19

Section 6: Security Measures ......................................................................... 20

6.1 Description of Security Levels 1 – 2 – 3 ....................................................... 20
6.2 Records of Dangerous Goods ...................................................................... 20
6.3 Restricted or Vulnerable Areas .................................................................... 20
6.4 Security Instruction from Contracting Government at Security Level Three .................................................. 21
6.5 Use of Fire Arms ............................................................................................ 21
6.6 Security Measures at Security Level One ..................................................... 21
6.7 Security Measures at Security Level Two ..................................................... 22
When using this template each page shall be clearly marked with the wording

Confidential

6.8 Security Measures at Security Level Three ........................................................................................................... 22

Section 7: Security Training, Drills and Exercises ....................................................................................................... 23

7.1 Training ......................................................................................................................................................... 23
7.2 Drills .............................................................................................................................................................. 24
7.3 Exercises ....................................................................................................................................................... 24

Section 8: Emergency Preparedness at Security Incidents .......................................................................................... 25

8.1 Security Incident and Provisions for Maintaining Critical Operations ................................................................. 25
8.2 Evacuation and Preparation for Evacuation .................................................................................................... 25
8.3 Searching and Contact Information to Experts .............................................................................................. 25
8.4 Bomb and Other Security Threats .................................................................................................................. 25
When using this template each page shall be clearly marked with the wording **Confidential**

### Annexes

<table>
<thead>
<tr>
<th>Annex</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex A</td>
<td>Security Assessment Report</td>
</tr>
<tr>
<td>Annex B</td>
<td>Access Control Procedures</td>
</tr>
<tr>
<td>Annex C</td>
<td>Management of Restricted Areas</td>
</tr>
<tr>
<td>Annex D</td>
<td>Instructions for Security Patrols</td>
</tr>
<tr>
<td>Annex E</td>
<td>Instructions for the use of CCTV Equipment</td>
</tr>
<tr>
<td>Annex F</td>
<td>Notifiable Incidents Instructions and Reporting Form</td>
</tr>
<tr>
<td>Annex G</td>
<td>Copy of the Statement of Security Compliance issued by (Details of issuing Authority)</td>
</tr>
<tr>
<td>Annex H</td>
<td>Training Record Form</td>
</tr>
<tr>
<td>Annex K</td>
<td>Emergency Evacuation Plan</td>
</tr>
<tr>
<td>Annex L</td>
<td>Security Threats</td>
</tr>
</tbody>
</table>

(Insert relevant documents relating to security as annex’s to the plan. These must be referred to in the appropriate section of the plan)
Document Status and Revision Control

Guidance:
Use the table on the front page of the Security Plan to record document status and revision control.

Purpose and Background

Guidance:
This security plan is written in accordance with the requirements of (Insert details)

This plan contains all the necessary information, operational procedures and measures required to protect vital surface transport infrastructure.

The security plan is based on a security assessment carried out on (Insert date) by (Insert details), a copy is attached at Annex ?? The plan will be updated and revised regularly and changed upon alterations to the infrastructure or nearby areas. The plan will also be reviewed in response to any security incidents.

Security measures are based on a plan of actions identified during the security assessment and in cooperation with local authorities and facility owners/operators. The plan further describes measures to be implemented at security levels 1, 2 and 3.

The purpose of this plan is to:

- Document and describe responsibility, measures and procedures for security of (Insert details)
- Establish routines for sharing of responsibility for security tasks between the relevant authorities responsible for the operation of the infrastructure.
- Act as guidance for the person responsible for security, with regards to security, in order to improve awareness, prevention and response to security incidents and threats.
- Give contact information to the relevant authorities and other security organisations.
- Through implementation and follow up of the plan, enhance the infrastructure security in order to identify, delay or possibly avoid security incidents.
- Ensure that the necessary records of security activities are kept for traceability and handling of non-conformities and maintained for audit purposes.
Definitions, Expressions and Abbreviations

Guidance:

**Infrastructure Security Officer**: The person designated by the relevant authorities for ensuring that a security assessment is carried out; that a security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with relevant authorities and Government Agencies.

**Infrastructure Vulnerability Assessment**: Process for assessment of an infrastructure elements vulnerability with regards to a security incident. A security assessment shall include the necessary measures relevant to the nature of the asset to be protected.

**Site Security Officer**: The person designated as responsible for the development, implementation, revision and maintenance of the security plan and for liaison with the relevant local authorities and law enforcement agencies for each individual site forming part of the asset to be protected. (i.e. Either side of a bridge or tunnel)

**Infrastructure Security Plan**: A plan developed to ensure the application of measures designed to protect the infrastructure, persons from the risks of a security incident.

**Security level 1**: The level for which minimum appropriate protective security measures shall be maintained at all times. Also known as “near normalcy”.

**Security level 2**: The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

**Security level 3**: The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target. It is envisaged that at level 3 outside assistance, such as provided by national security or military services, will step in and take control of the ongoing situation.

Section 1: Infrastructure Details

**Name of Infrastructure:**

(Insert details)
When using this template each page shall be clearly marked with the wording
Confidential

Name of Operating Company/Department:
(Insert details)

Full Postal Address:
(Insert details)

Telephone and Details:
(Insert relevant telephone numbers giving 24 hour contact details)

Fax
(Insert fax numbers identifying which are 24 hour)

Nominated Security Officer:
(Name of person nominated as facility Security Officer)

Security Training Course Successfully Completed:
Date: June 2005
Location: ??
Training Provider: (Insert details)

Security Officer Contact Details:
Postal Address:
(Enter contact details for nominated security officer ensuring 24 hour contact)

Telephone: 

Fax: 

Mobile: 

E-Mail: @

Deputy Security Officer:
(Enter name of nominated Deputy Security Officer)

Security Training Course Successfully Completed:
Date: (Insert details)
Location: (Insert details)
Training Provider: (Insert details)

Deputy Security Officer Contact Details:
(Enter contact details ensuring 24 hour coverage)

Postal Address:
(Insert details)
When using this template each page shall be clearly marked with the wording
Confidential

Telephone: +
(Enter relevant telephone numbers ensuring 24 hour contact)

Fax: +

Mobile: +

E-Mail: @

Name of Senior Manager to whom Security Officers Report:
(Insert details)

Date Security Plan submitted for approval:
(Insert date the plan was submitted to the competent authority for approval)

Date Security Plan approved by competent authority:
(Insert the date plan received approval from the competent authority)

Dates any amendments submitted for approval:
(Insert dates any amendments were submitted to competent authority for approval)
Section 2: Protection of Security Related Information

2.1 Classification and Protection of the Security Plan

The Infrastructure Security Plan and its attachments are classified Confidential or Restricted documents. Distribution is limited to those persons who have a responsibility to implement all or part of the plan. The information contained in the plan is highly sensitive and could seriously harm the supply chain security position if disclosed to unauthorised persons.

Where persons have a responsibility to implement a specific part of the plan they will only be issued with the relevant Annex containing their instructions in order to fulfil their duties.

2.2 Access to the Security Plan

Only authorised persons will have access to the plan. Copies of the plan will be numbered and issued to those listed below:

<table>
<thead>
<tr>
<th>Copy No</th>
<th>Job Title</th>
<th>Name</th>
<th>Contact No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 Safeguarding of Security Related Information

In addition to this plan other information related to security also requires protection this includes:

- (Enter information relating to security of the infrastructure that needs to be protected)

All staff with a responsibility for handling security related information have received training in information management. This is recorded in their training records held by (Insert name and appointment of person holding training records)

Hard Copy Information Transfer and Storage

- When not in use, Classified and/or Confidential information must be stored in locked drawers, cabinets, or rooms specifically designated for that purpose and that are accessible only by authorised individuals.

- When transferring hard copy Classified information, documents shall be placed in envelopes and sealed with the name of the intended recipient and the words "Classified Information" clearly marked. This envelope shall
When using this template each page shall be clearly marked with the wording **Confidential**

be placed in another plain envelope, (envelopes normally used for internal and external mail are acceptable if they meet the criteria) sufficiently opaque to hide the sensitive nature of the information contained within and contain the return address of the sender.

**Use of Copiers and Area Printers**

- Printers and copiers must not be left unattended when Classified or Confidential data is being printed or copied.

- Networked printers are accessible to anyone on the network and are known to have vulnerabilities that allow unauthorised users to read, modify, or delete the information. Therefore, Classified data must be printed only on printers approved and designated for this level of data. This requirement applies to each individual printer and not to entire printer classes.

**Fax Transmissions**

- The fax machine is to be kept in a secure area, the fax machine must not be unattended when Classified or Confidential information is being faxed.

- Information sent via fax must include a Company fax cover page with a disclaimer that the information sent is for the use of the intended recipient only.

**Hard Copy Disposal**

- All Classified or Confidential information in hard copy form must be either shredded or incinerated when being disposed of. Rubbish containers or recycling bins are not appropriate means of disposal of the above levels of information. It is the responsibility of the user in possession of the hard copy information to ensure that proper disposal occurs.

**2.4 Safeguarding Electronic Information**

The electronic storage of security related information conforms to Best Practice standards of access to electronically stored information. There should be in place:

- ID Password Only Accessibility
- Levels of Authorised Accessibility
- Supervisory Level Administrator
- Local Area Network with controlled access
- Firewalls

(Add any additional local requirements for protecting electronic information)
Section 3: Internal/External Audit, Review and Updating of the Security Plan

3.1 Internal Audit

The plan will be constantly under review by the Security Officer to ensure that it continues to meet the needs of the Supply Chain Security infrastructure requirements. Any inadequacies will addressed without delay. The Security Officer will arrange for an internal audit once every 6 months on elements of the plan.

3.2 External Audit

The Security Officer will be responsible for ensuring that external audits of the facility are conducted annually to ensure the integrity of the security plan and procedures.

3.3 Review and Updating of the Security Plan

The Security Plan will be treated as a living document. The plan will be reviewed on an annual basis and following any breach of security, security incident or information gained from audit.

The annual audit will be conducted by an independent organisation to ensure that the standards required by the plan are being maintained.

3.4 Approval of Updates

Any amendments to the plan or procedures must be approved by the relevant authorities before they are implemented. Once amendments have been approved they will be circulated to all holders of the relevant security procedure. A confirmation card will be sent with the procedure to ensure that all persons requiring the information receive it and amend their security procedures accordingly.

It will be the responsibility of the Security Officer or his Deputy to confirm this is completed and that the Security Officer receives confirmation that the amendment has been implemented.

Any amendments that fundamentally alter the plan will be submitted to the relevant authorities for their approval prior to implementation.

3.5 Reporting of Security Incidents or Breaches of Security
When using this template each page shall be clearly marked with the wording **Confidential**

All security incidents or breaches of security will be reported to the Security Officer who will report to the relevant authorities. The Security Officer is to ensure that a follow up investigation is conducted, and the results will be recorded and submitted to the relevant authorities.

Incidents or breaches of security that are contained on the list of reportable incidents are to be reported to the relevant authorities who will, if required, report it to the Government Department. *(Note: Each member state will have its own security rules)*
Section 4: Management of Security

4.1 Responsibility for Transport Infrastructure Security

The overall responsibility for the security of the infrastructure asset rests with the Security Officer and ultimately the relevant authorities. They will individually or together, make decisions that, in accordance with their professional judgement, are required for maintaining the security of the infrastructure asset. This includes initiation of any measures required or necessary to maintain the security of the infrastructure and other assets.

The duties and areas of responsibility of the Security Officer and the relevant authorities shall include but are not limited to:

- Performance of a comprehensive initial security survey of the transport infrastructure and other assets to assess the current levels of security. The results of the survey will be used to produce a Infrastructure Security Plan for the *(Insert details)*

- To ensure the development and maintenance of the Security Plan. The plan should be viewed as a living document and constantly reviewed to ensure it continues to meet the needs of the operation.

- Conduct periodical security inspections of the Transport Infrastructure in order to ensure the security plan is being implemented correctly.

- Recommend and include modifications to the Security Plan in order to improve weaknesses and update the plan so that changes to the facility security are implemented.

- To raise security awareness amongst all employees involved in the management and maintenance of the Transport Infrastructure Asset.

- Ensure that adequate training is offered to personnel with security responsibilities.

- Report to the authorities and keep records of security threats to the Transport Infrastructure.

- Coordinate the implementation of the Security Plan with sub contracting companies.

- Ensure that employees responsible for security of the Transport Infrastructure Asset adhere to the relevant standards.

- Ensure that security equipment is correctly used, tested, calibrated and maintained.
Other Company and Contractor personnel have responsibility for aspects of security within their job function these include:

Local Law Enforcement Agencies
Local Authorities
National Authorities

These personnel are responsible for:

Local Law Enforcement Agencies:

- (Insert details)

Local Authorities:

- (Insert details)

- 

National Authorities:

- (Insert details)

- 

4.2 Details of security contractors (if used) and their contracted duties:

Private Security Staff are employed and carry out the following duties:

- (Enter details of the duties carried out by private contractors in relation to security)

Regular training is given to all members of the security team to ensure they maintain their skills, are informed of new procedures and remain current and informed about local conditions.

Private Security Contractors are monitored by (Enter name and appointment of person monitoring security contractors) to ensure they maintain the standards set by (Insert details of legislation/local rules governing the work of security contractors).
4.3 Security Level Changes

Procedures for receiving and disseminating Security Level Information to relevant staff:

Any change to the security level received by the Transport Infrastructure Management from the Government or other relevant authorities will be passed immediately to the Security Officer or his deputy. This information will then be authenticated by the Transport Infrastructure Administration before being disseminated to other personnel responsible for implementing any additional measures that need to be taken. *(Include contact information of persons responsible for disseminating security information and instructions showing how this will be achieved in a secure manner.)*
4.4 Security Organisation Chart

(Insert a flow chart clearly showing the organisation of the infrastructure security assets)

![Flow Chart]

Government Department

Relevant Authority

Transport Control

Law Enforcement  Security Patrols

4.5 Response to and Reporting of Security Threats, Incidents and Breaches of Security

Response to a security incident:

The member of staff discovering or receiving the information concerning a security incident will report the details immediately to the Security Officer. If the incident is serious it will be reported without delay to the Local Law Enforcement Agencies. The initial response will be the implementation of the relevant security procedure that best suits the incident / threat that has occurred.

Recording procedures:

All security incidents, threats, breaches and visits will be recorded in the security log held by (insert details of the person responsible for maintaining the security log) located in the (insert location of where security log is located)
On receiving information of an incident, threat or breach of security *(Insert name and appointment of person responsible)* is to maintain a chronological account of the incident in the security log.

**Security incident investigation procedures:**

All security incidents are to be investigated by the Security Officer or person designated by the authorities. All persons involved in the incident are to be interviewed and their account of the incident recorded. This should be conducted as soon after the event as possible to ensure information is gathered whilst it is fresh in people's minds. Once the investigation is complete a full report is to be prepared. Where necessary a copy of the report will be forwarded to the relevant government authorities for their information and action.

Information gained from any investigation is to be used to update the Assessment, Plan and Procedures as necessary.

**Reporting procedures for reporting to government agencies:**

Notifiable incidents as defined by the Government Agencies are to be reported without delay using the report form attached at Annex ?? of this plan.

**4.6 Security Equipment**

The following security equipment is deployed at the Transport Infrastructure Asset:

- *(Insert details of all security equipment that is available at the infrastructure location)*

Equipment is checked monthly by *(Insert name and appointment of person responsible for checking security equipment)* as required and any faults are reported to *(Insert name and appointment of person responsible for ensuring repairs are carried out)* who arranges for repairs to be carried out. Repairs and calibration when required are conducted by the Maintenance Department or a designated contractor.
Section 5: Interface with Relevant Agencies

5.1 Exchange of Information

The exchange of information between the Transport Infrastructure Management, Government Departments and Law Enforcement Agencies forms a vital part of the security plan. In order to ensure that the best possible security measures are implemented all parties must be clear as to what they are expected to have in place. This will provide confidence to all parties that the best possible deterrents are in place to protect the Transport Infrastructure Asset.

5.2 Coordination of Security Measures

It is in the interest of all parties that the Transport Infrastructure Management and relevant Government and Law Enforcement Agencies work together to ensure the best level of security protection for all Transport Infrastructure Assets.

In normal circumstances no one other than essential personnel are allowed to visit the non public areas of the Transport Infrastructure Asset. However, should it be agreed that this may take place the Security Officer will provide to the Asset Management a list of persons who are expected to visit. This list will be held at the entrance and the visitors subjected to the normal access requirements as contained in Annex ??.
Section 6: Security Measures

6.1 Description of Security Levels 1－2－3

Security level 1: The level for which minimum appropriate protective security measures shall be maintained at all times. Also known as “near normalcy”. When at this level the Transport Infrastructure Asset Security Standing Operational Procedures will apply.

Security level 2: The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident. The actions to be taken at this level are contained within the procedures attached as Annex’s to this plan.

Security level 3: The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target. It is envisaged that at level 3 outside assistance, such as provided by national security or military services, may step in and take control or assist with the ongoing situation.

The security Level is set by the Relevant Government Department and sets the minimum standard that must be implemented within the Transport Infrastructure. However, the asset may if it wishes implement a level higher than that set by the Government in order to protect the facility.

6.2 Records of Dangerous Goods

Dangerous goods areas are a potential hazard to the security of the Transport Infrastructure Asset. It is important that dangerous goods are controlled and stored under secure conditions. All dangerous goods stored within the asset boundaries are stored at (Insert details of where dangerous goods are to be stored) under controlled conditions. The person responsible for the management of dangerous goods is (Insert name and appointment of person responsible for the management of dangerous goods).

6.3 Restricted or Vulnerable Areas

The following areas have been designated as Restricted Areas:

- (Insert details of Restricted or Vulnerable areas that were identified during the security assessment)

Full details of how this area will be protected at Security Levels one, two and three are contained in Section 6 of this plan.
6.4 Security Instruction from Contracting Government at Security Level Three

When security level three is implemented by the Government Department responsible all elements that apply to security level two will be implemented. If the threat is a specific threat to the asset a crisis management team will be assembled to manage the situation.

Access to the non public areas of the Transport Infrastructure Asset will be restricted to full pass holders. Vehicular movement in and out of the non public areas will be kept to emergency requirements only. All access to and egress from the asset will be made via the (Insert details of relevant entry points) entrance. All persons and vehicles entering the non public areas will be subjected to a 100% identity check and security searches. In addition random security checks and searches may be conducted within the public access areas.

In addition to the above, staff will implement any requirements or instructions that are issued by the relevant Government Agencies.

6.5 Use of Fire Arms

Insert National Rules for the carriage of fire arms by security personnel

6.6 Security Measures at Security Level One

The security measures at level one address the following activities:

- Site Access
  - Annex B

- Restricted Areas
  - Annex

- Etc (Insert details of any other relevant activities identified during the security assessment)

- Monitoring Security of the Transport Infrastructure Asset
  - Security Patrols  
    - Annex ??
  - CCTV
  - Security Lighting
  - Etc
6.7 Security Measures at Security Level Two

The security measures at level two address the following activities:

- Site Access
  - Annex B
- Restricted Areas
  - Annex
- Etc
- Monitoring Security Within The Port Facility
  - Security Patrols
    - Annex ?
  - CCTV
  - Lighting
  - Consideration will be given to increasing the frequency of security patrols
  - Etc

6.8 Security Measures at Security Level Three

The security measures at level three address the following activities:

- Site Access
  - Annex B
- Restricted Areas
- Etc
- Monitoring Security Within The Port Facility
  - Security Patrols
  - CCTV
  - Lighting

- Etc
- In addition to the above actions at Level three Transport Management staff will respond to instructions given by the relevant Government Department or Law Enforcement Agencies with regard to the actions required at this level to counter the perceived threat.
Section 7: Security Training, Drills and Exercises

7.1 Training
The Security Officer, Security Personnel and other staff with security responsibilities should have knowledge of and receive training in all relevant areas of their security duties:

(Identify training needs and requirements and complete grid below to meet the needs of the infrastructure organisation)

<table>
<thead>
<tr>
<th>Security Officer</th>
<th>Security Personnel</th>
<th>Other personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relevant international conventions, codes and recommendations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relevant Government legislation and regulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsibilities and functions of other security organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methodology of asset security assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency preparedness and response and contingency planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling sensitive security related information and security related communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge of current security threats and patterns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition and detection of weapons, dangerous substances and devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security of the facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Techniques used to circumvent security measures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security equipment and systems available at the facility and their operational limitations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methods of conducting audits, inspection, control and monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methods of physical searches and non-intrusive inspections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security drills and exercises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment of security drills and exercises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations of security equipment and systems available at the facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing, calibration and maintenance of security equipment and systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security related communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methods of physical searches of persons, personal effects, baggage and vehicles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The meaning and the consequential requirements of the different security levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc (Add any further local requirements)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All training is to be recorded using the document contained at Annex ?? It should also be entered into the individuals training records held by (Insert details of person who manages training records)
7.2 Drills

Drills are an important element in ensuring that all staff are practiced and confident in their responsibilities and reactions to a security related incident.

In order that staff remain current a series of drills will be carried out at specified intervals to ensure that all elements of the organisation are tested and reviewed at least annually.

A record of all drills conducted is to be maintained in the security log and retained for audit purposes.

Shown below are the drills that are planned and the interval of frequency:
(Asend as applicable)

<table>
<thead>
<tr>
<th>Drill (Name/Purpose)</th>
<th>Method</th>
<th>Frequency</th>
<th>Responsible</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Training for supervisory positions</td>
<td>Formal Training</td>
<td>Annually</td>
<td>Security Department/Consultant</td>
<td>??</td>
</tr>
<tr>
<td>Suspect device at transport infrastructure</td>
<td>Practical drill</td>
<td>Quarterly</td>
<td>??</td>
<td>??</td>
</tr>
<tr>
<td>Unauthorised persons in a restricted area</td>
<td>Practical drill</td>
<td>Six Monthly</td>
<td>Security Officer</td>
<td></td>
</tr>
<tr>
<td>Total Facility evacuation</td>
<td>Table Top</td>
<td>Annually</td>
<td>Security Officer</td>
<td></td>
</tr>
</tbody>
</table>

7.3 Exercises

(As depending on the nature of the facility several types of exercise could be conducted involving all agencies with a role to play. These may be police, fire, ambulance, environmental, military etc. This section needs to give details of how these are conducted and who they involve. As an example the Channel Tunnel closes for 12 hours once per year to allow multi agency exercises to take place to ensure all parties are practiced in their particular disciplines which may have been practiced as individual drills at other times. It ensures that all events are coordinated and that conflicts of interest do not occur.)
Section 8: Emergency Preparedness at Security Incidents

8.1 Security Incident and Provisions for Maintaining Critical Operations

Instructions for the management of incidents within or adjacent to the Transport Infrastructure Asset are contained within the Asset Emergency Manual a copy of which is attached at Annex ? to this plan.

(Need to be updated to include Security Incidents, Emergency Plan)

8.2 Evacuation and Preparation for Evacuation

In the event that an evacuation of the complete asset is required the Evacuation Plan will be implemented. A copy of the plan is attached at Annex ?? (Insert Copy of the Evacuation Plan, does one exist, does it cover Security Incidents??)

If a partial evacuation is required the area will be cleared and cordoned by the (Insert details of who is responsible) whilst the incident is dealt with by the incident controller.

(What procedures exist for evacuation for a security incident within the transport asset??)

8.3 Searching and Contact Information to Experts

(Need to establish contact details of government agencies that can assist with specialist search and expert assistance such as EOD, Clearance Divers etc. What Search Plans do we have in place i.e. Bomb threat searches etc) Who is this arranged by??

8.4 Bomb and Other Security Threats

The procedure for handling bomb threats is contained in the following Annex:

- (Insert details) Annex ??
Report Appendix C: Current Initiatives
It is imperative that new legislations which are being developed to improve security of the supply chain within the EU shall connect, where possible seamlessly, with existing initiatives or initiatives in progress to prevent duplication of efforts and cost escalating effects for trade and industry.

Airborne and maritime transports have established security regimes and also the transportation of dangerous goods has become subject to security requirements since the beginning of 2005.

Traditionally, security Management of the land based supply chain only addressed the prevention of theft and damage of cargo. An example of this is the certification program that has been developed by TAPA (Technology Asset Protection Association). The attack on the WTC on September 11 2001, however, has increased the focus on supply chain security which has resulted in a number of national and international initiatives.

Recent supply chain security initiatives have been (or are being) developed and implemented by customs organisations because these are historically responsible for supervising the international flow of goods for compliance to import duty and health and safety regulations. This so far has resulted in a number of different supply chain security requirements. Apart from requirements to the management of supply chain security these customs driven regulations have one common requirement. Customs want to have advanced information on the character of cargo that is entering their jurisdiction in order to decide which cargo they will target with intensified inspections, based on a risk assessment. The World Customs Organisation is attempting to establish an umbrella which should harmonise these customs regulations on security management and advanced cargo information to facilitate international trade.

In response to the lack of a consistent set of standards for supply chain security the industry has taken matters in its own hands. Whereas individual companies started to develop their own systems, and so setting their own standard in the market, ISO has taken the initiative to start developing a set of ISO documents which should fulfil the needs of industry and so establish a better regulated and harmonised set of requirements to supply chain security.

1. The International Shipping and Port Facilities Security (ISPS) code

One of the measures introduced, and with a global impact on international trade has been the implementation of the ISPS-code which formulates requirements to security management in international shipping and at port facilities (see also report 2). The ISPS code is anchored in the SOLAS convention, as administered by the International Maritime Organisation (IMO), which ensures global enforcement of the code by all flag- and port states.

The correct implementation of the ISPS code on board ships is being verified and certified by the flag states, where most flag states have delegated this to Recognised Security Organisations i.e. a limited number of classification societies. The certification of the world fleet was completed on the deadline being 1st July 2004.

Verification of implementation of the ISPS code at port facilities is done by national authorities. Different countries have chosen different approaches and IMO has been venting its concern on both the progress and the consistency of this verification. Reason for the delays in implementation is that some ports are extremely difficult to secure because they are integrated in the infra-
structure of cities, which makes compliance to the code not only time consuming but also very expensive.

2. Aviation

At the time of the terrorist attacks on WTC on September 11, 2001 there were already European Regulations in the field of aviation security for all EU Member States, which were superseding the various national laws. These were the result of various hijack of aircraft and airport attacks in the 70’s. But after the WTC disaster the attention and focus on aviation security increased rapidly. This resulted within the EU in a number of new Regulations in this field. The most important regulation is definitely Regulation 2320/2002, establishing common rules in the field of civil aviation security. The Regulation is based on the (international) ICAO Annex 17 standard, European Civil Aviation Conference recommendations and Commission proposals.

After the already mentioned above Regulation 2320/2002 a variety of aviation security focused regulations have been established. These additional Regulations are mainly harmonising the implementation of Regulation 2320/2002 and are addressing issues like security quality control programmes, conducting Commission inspections and security restricted areas.

The Regulations are applicable to:
- All EU airports.
- All service providers at those airports.
- All cleaning and catering providers.
- All cargo parties.
- All airlines both EU and foreign departing or transiting to any EU airport.

Regulation 2320/2002 provides common standards and detailed rules in the following areas:
- Airport Security, including access control and 10% staff screening
- Aircraft Security, including aircraft inspections and protection of aircraft when in and out of service
- Passenger and cabin baggage screening
- Hold baggage screening and protection
- Cargo, courier and express parcels, including detailed rules on handling, screening and protection of cargo
- Company mail and materials
- Public mail
- Air carrier catering and cleaning and their stores and supplies
- General aviation
- Staff Recruitment and training
- Equipment standards
3. Transport of dangerous goods

3.1. International Carriage of Dangerous Goods by Road (ADR)

The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR) was signed at Geneva in 1957 under the auspices of the United Nations Economic Commission for Europe, and it entered into force in 1968.

The Agreement addresses in great detail the safety of the road transportation of dangerous goods.

As from the 1st of January 2005 a completely revised Agreement has been in force. Recognising the fact that terrorists can cause massive atrocities with dangerous goods, transported by road, i.e. a new Chapter 1.10 has been added which specifies a number of security measures to be taken.

These measures include training of personnel, security policies, operating practices and equipment (serving f.i. theft prevention) and resources, which shall be documented by the operator in a security plan.

3.2. International Carriage of Dangerous Goods by Inland Waterways (ADN)

The International Carriage of Dangerous Goods by Inland waterways (ADN) was adopted in 2000 on the occasion of the Diplomatic Conference organized jointly by the Economic Commission for Europe (UNECE) and the Central Commission for the Navigation of the Rhine (CCNR).

ADN consists of a set of safety related requirements and does not address security issues. The ADN is applicable as from 1 January 2005 as ECE/TRANS/182

3.3. Transport of dangerous goods via rail

Annex 1 to the Convention concerning International Carriage by Rail (COTIF), defines Regulations concerning the International Carriage of Dangerous Goods by Rail (RID) which came into force in 1985 and only addresses safety issues.

In the UK the security of transport of dangerous goods via rail is regulated by a voluntary code of practice which is enhancing the security of UK railways. It makes good use of the measures recently agreed in RID and offers practicable and relevant guidance. Its implementation reduces the vulnerability of the UK to a successful terrorist attack.

4. Customs-Trade Partnership Against Terrorism (C-TPAT)

Shortly after 9/11, US Customs has begun work with US industry (under the Customs-Trade Partnership Against Terrorism - C-TPAT programme) to certify companies that have secure supply chains, to increase security and to facilitate processing. The C-TPAT program is a voluntary partnership between U.S. Customs and the U.S. import trade community to reduce threat risks. The objective of C-TPAT is to strengthen and fortify the supply chain importing into the US against terrorism and to balance needs for such increased security measures in con-
junction with a reduction in unnecessary delays due to customs intervention for legitimate and compliant trade.

Participation in the C-TPAT program requires from importers to:

- Submit an application to Customs to obtain approval in order to participate.
- Submit a supply chain security questionnaire to Customs.
- Develop and implement a program to enhance security where they have control throughout the supply chain.
- Communicate their C-TPAT guidelines in areas where they do not have control, to other companies in their supply chain that do have control and work towards building secure relationships with these companies.

The program requires importers to ensure the integrity of their security practices and to communicate security guidelines to their business partners at each segment of that supply chain: production, transportation, importation, and distribution. Joint cooperation between all parties involved: importers, brokers, manufacturers, warehouse operators, air-carriers, ocean-carriers, and land-carriers; is crucial. Currently, applications to become a C-TPAT member are being accepted from the following groups:

- Importers
- Carriers (air, sea and land)
- Customs Brokers
- Air Freight Consolidators
- NVOCs (Non-Vessel Operating Common Carriers)
- Ocean Transportation Intermediaries
- Highway Carriers
- Selected Foreign Manufacturers

At a minimum, the following security elements need to be addressed:

- Physical Security
  - Measures in place to protect the physical security of facilities and conveyances.
  - Measures that are in place to prevent theft of goods at premises or while in transit
  - Measures that are in place with respect to shipping and receiving controls
  - Measures that are in place to protect automated systems
  - Description of the security program’s internal controls and method to report and correct problems.

- Personnel Security
  - Pre-employment screening, recruiting practices and periodic background checks that are conducted on employees.
  - Description of training which employees are given on security awareness and procedures.
  - A policy regarding security violations
  - Internal controls which are in place for reporting and managing problems related to personnel security?

- Service Provider Requirements
o Security standards which do you apply to protect property, conveyances and freight when employing service providers?

o How to include major service providers and international trade chain partners in enhanced security measures

Membership is not restricted as to nationality. Any business entities within the above groups who may be foreign owned yet import commercial goods to the United States are eligible.

5. Partners in Protection (PIP)

Partners in Protection (PIP) is designed by Canadian customs, as the equivalent to C-TPAT, to promote the co-operation with private industry in efforts to enhance border security, combat organised crime and terrorism, increase awareness of customs compliance issues, and help detect and prevent contraband smuggling.

Organisations sign a partnership agreement with the Canada Border Services Agency (CBSA), which is based on goodwill. Industry and the CBSA work together focusing on security, the exchange of information, and awareness. Like C-TPAT this program is also based on self-assessment to identify weaknesses in security processes. The goal is to minimise the threat of illegal activity. Organisations that demonstrate their commitment to a secure trade chain by joining PIP will be eligible to participate in the Free and Secure Trade Program (FAST). FAST makes cross-border commercial shipments simpler and subject to fewer delays, all while enhancing security.

6. Free and Secure Trade (FAST) program

The Free and Secure Trade (FAST) program is a joint Canada-U.S. initiative involving the Canada Border Services Agency, Citizenship and Immigration Canada and the United States Bureau of Customs and Border Protection (CBP). FAST supports moving pre-approved eligible goods across the border quickly and verifying trade compliance away from the border. It is a harmonised commercial process offered to pre-approved importers, carriers, and registered drivers. Shipments for approved companies, transported by approved carriers using registered drivers, will be cleared into either country with greater speed and certainty, and at a reduced cost of compliance. FAST is available to those participants who have a demonstrated history of compliance with all relevant legislation and regulations, and have acceptable books, records and audit trails.

A unique feature of the FAST program is that it is the only program to date which also contains the aspect of personnel certification. Truck drivers may qualify to participate in the program if they are a citizen or permanent resident of the U.S. or Canada, age 18 or over and possess a valid driver’s license. They must be admissible to Canada and the U.S. under applicable immigration laws. However, they may not qualify if they:

- provide false or incomplete information on their application;
- have been convicted of a criminal offence;
- have been found in violation of customs or immigration law; or
- fail to meet other requirements of the FAST Commercial Driver Program.
The driver must provide his employment history for the last five continuous years. Under the program a full set of fingerprints is taken to perform criminal records checks, which together with other will be shared with other government and law enforcement agencies. Participation in this program is strictly voluntary and valid for a five-year period.

Canadian or US privacy legislation is applicable and information shall only be shared with the relevant law enforcement agencies. Under the provision that the driver agrees his participation in the FAST program is communicated to outside parties.

7. StairSec®, the security part of the Swedish Stairway program

StairSec is targeted towards practical solutions in order to establish an authorised secure supply chain for all stakeholders in the international supply chain, namely importers/exporters, brokers, forwarders independent of transport mode and also terminals, such as seaports, warehouses and other hubs for cargo management.

It refers to itself as a quality assurance programme which builds on separate modules for:

- Exporters/importers
- Brokers
- Forwarders
- Terminals

Compliance to the requirements is assessed by Swedish customs themselves which results in far-reaching facilitation in terms of decreased control levels for certified companies. The requirements in StairSec are very similar to those of C-TPAT and a close cooperation between Swedish and US Customs has been developed.

8. Secure Trade in the APEC Region (STAR) initiative

Under leadership of the US, the 21 Member States of APEC have agreed on the Secure Trade in the APEC Region or STAR initiative. This is a voluntary scheme which the individual countries implement over time. To enable this Private Sector Supply chain Security Guidelines have been developed. Key features of the STAR initiative include i.e.:

- a container security regime for goods;
- strengthened cooperation between governments and the private sector to secure the supply chain for goods;

The requirements, formulated in the guidelines are very similar to C-TPAT. In order to secure their exports to the US and not to get disconnected with the rest of the industrialised world both Australia and New Zealand have turned the STAR initiative into concrete programmes.

Australia’s Frontline and Accredited Client Program

Unlike the aviation and maritime industries, where security legislation is the primary responsibility of the Australian Government, surface transport security, including rail, light rail, buses, and passenger ferries, is the responsibility of the state or territory in which the service is lo-
cated. The Australian Government's role is to work with state and territory governments to develop a consistent and coordinated approach to surface transport security. They are preparing an intergovernmental agreement which shall provide guidance to the different jurisdictions and the transport industry.

Items on the work program include:

- Preparing guidance material for service operators on a range of topics, including a guide to undertaking a security risk assessment, a guide to preparing a security plan, and an unclassified version of relevant threat assessments. Copies of this material can be found below.
- The development of a nationally consistent approach for the security regulation of dangerous goods.
- Developing a yearly forum program for service operators and government officials working in transport security - the first forum, focusing on urban mass transport, will take place in mid 2005.

New Zealand

New Zealand has implemented the Secure Export Partnership, a voluntary cooperation scheme between Customs and industry, based on a set of supply chain security management measures which are quite specifically defined.

The Secure Export Partnership scheme sees security issues sorted out prior to loading by:

- Customs performing audits on companies to verify compliance with the requirements of the Secure Export Partnership.
- Customs performing inspections on cargo before it is shipped and enters the supply chain

The scheme is a key element of Customs' supply chain security strategy, which forms the basis of an arrangement between the US and New Zealand Customs administration. The Secure Exports Partnership means that both the company and Customs can have confidence its goods are secure from the point of pack to the port or airport.

More than 50 exporters have qualified as Secure Export Partners. The scheme requires businesses to have robust security measures in place to ensure export goods cannot be tampered with or used to smuggle contraband. At the point of packing for export, the consignment of goods is sealed with a Customs-approved seal, signalling that it is under Customs control and can be considered secure by overseas administrations. While the scheme is voluntary, Customs control over the sealed consignments is legislated for in the amended Customs and Excise Act.

9. WCO Framework of Standards to Secure and Facilitate Global Trade

The World Customs Organisation was requested in 2003 by both the G7 and IMO to develop supply chain security instruments for the non-maritime part of the supply chain. In response to this request the WCO installed a security task force which worked on a basis of consensus between custom organisations and trade and industry. This security taskforce has developed standards for advanced cargo information and standard data elements on cargo documentation.
In addition, based on the work of the security taskforce, WCO has established a High Level Strategic Group, comprising a small, diverse group of Directors General, who are committed to security and facilitation. This group has established a Framework of Standards to Secure and Facilitate Global Trade. This Framework has the objective to harmonise the approach which different customs administrations take towards cooperation, mutually between customs organisations and between trade and customs, recognizing the needs of both industry and the customs administrations. This framework is expected to be adopted by the WCO Council meeting in June 2005 and is based on 2 series of standards.

The pillar 1 standards describe the interaction between customs organisations. It set a number of broad standards for:

- Integrated Supply Chain Management
- Cargo Inspection Authority
- Modern Technology in Inspection Equipment
- Risk-Management Systems
- High-risk Cargo or Container
- Advance Electronic Information
- Targeting and Communication
- Performance Measures
- Port Security Assessments
- Employee Integrity
- Outbound Security Inspections

The broad standards from pillar 1 are further detailed in an Annex 1 to the Framework for standards, defining technical specifications which among other things provide a clear definition of the Authorised Economic Operator (AEO). To this Annex 1 an Appendix has been developed describing in detail the WCO Seal integrity Program.

The pillar 2 standards describe the interaction between customs and the private sector. It sets a number of broad standards for:

- **Partnership:** Authorized Economic Operators involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments until they are released from Customs control at destination.
- **Security:** Authorized Economic Operators will incorporate pre-determined security best practices into their existing business practices.
- **Benefits:** The Customs administration, together with representatives from the trade community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as Authorized Economic Operators. These processes will ensure that they see a benefit to their investment in good security systems and practices, including reduced risk-targeting assessments and inspections, and expedited processing of their goods.
- **Technology:** All parties will maintain cargo and container integrity by facilitating the use of modern technology.
- Communication: The Customs administration will regularly update Customs-Business partnership programs to promote minimum security standards and supply chain security best practices.
- Facilitation: The Customs administration will work co-operatively with Authorized Economic Operators to maximize security and facilitation of the international trade supply chain originating in or moving through its Customs territory.

The broad standards from pillar 2 are further detailed in an Annex 2 to the Framework for standards, defining technical specifications which among other things provide a number of supply chain security requirements. To this Annex 2 Appendices are under consultation which will specify more detailed requirements to:

- The management of supply chains security
- The validation processes custom organisations should apply

These issues are of a sensitive nature, because differences in interpretation and application will automatically lead to disturbance of the level playing field for trade.

The development and implementation of the above instruments has been and will be quite time consuming because WCO has no legislative power through which they can enforce their resolutions. Therefore WCO has opted to:

- Combine supply chain security requirements with trade facilitation measures (the carrot) which easily dilutes focus and results in mixed thinking process and discussions.
- Aim for consensus with trade who, even being of good will, has different interests it wants to defend
- Give facilitation to less developed parts of the customs community to ensure equal interpretation and implementation of its framework around the globe.

10. EU Revised Customs Code

The upcoming changes to the Community Customs Code are the most important since the Code was adopted in 1992. More specifically, the European Commission wants a radical overhaul of the customs rules, the purpose of which is to enable traders to save time and money in their transactions with customs. One of the keystones of the amendments to the Customs Code is the greater role for customs in managing security at the EU’s external borders.

One of the main innovations is that declaration will in the future have to be presented before the goods arrive at the EU border. In other words, a pre-notification system by means of pre-arrival declarations will be put in place. This will allow an adequate pre-screening of shipments and risk analysis, confirming the new role of Customs offices at the external borders, i.e. their focus on safety (cf. infra). On the other hand, goods destined to leave the Customs territory of the EU will have to be covered by pre-departure declarations.

Traders will have to comply with these requirements. This should lead, together with a harmonised risk assessment system of customs, to a tightened security around goods crossing the EU borders while not blocking the physical flow of goods because of faster and better targeted checks by Customs.
Within the scope of the current changes of the Community Customs code, the authorities have introduced the principle of ‘Authorized Economic Operator (AEO)’. The advantage of the AEO is that customs controls and the application for authorisations will be easier in the future. The status of AEO will be recognized by the customs authorities in all Member States. The criteria for recognition as AEO will vary from financial solvency, appropriate record of compliance with customs requirements to appropriate security and safety standards.

The standards for security are presently under development and are expected to be a combination of requirements as defined under the C-TPAT and the StairSec® programs.

11. Technology Asset Protection Association (TAPA)

The Technology Asset Protection Association (TAPA) was established in the US in 1997 and is an association of security professionals and related business partners from high technology companies who have the purpose of addressing the emerging security threats for the technology industry.

The development of the high tech industry in the 90’ies has had as a side effect that another sector in economy has been growing as well, namely the theft of high value goods. The prime objective of TAPA has been to reduce losses to industry due to criminal activities and as a consequence reduce insurance premiums.

In addition to the fact that security has been put high on the agenda with its member companies and that these companies have developed effective security management systems for securing their own operations TAPA has implemented two key initiatives to start this process:

- To draw up a set of agreed Freight Security Standards (FSR) to act as a guide to shippers of hi-tech freight on the standards of freight security required by the manufacturers. This is now being implemented across the World.
- To set up a common pool of information related to criminal activities against TAPA freight in transit - Incident Information Service (IIS). This information is stored centrally, constantly updated with new incident reports and along with other related information services is freely available to all TAPA members and relevant Law Enforcement.

The Freight Security Standards are the basis for a certification system. TAPA has nominated a number of third and second party auditors which perform assessments on in-transit storage and warehousing of any TAPA members’ assets throughout the world and who independently confirm if such suppliers comply with the FSR requirements. There exist 3 certification levels (A, B and C) which reflect the required degree of security, based on loss potential.

In 1999 TAPA-Europe (TAPA-EMEA) has been established and by now 30 multinational Europe based corporations, such as 3M, Hewlett Packard, Philips, Apple, Philip Morris, Samsung are member. Per today 49 facilities have been certified within the EU.

12. American Society for Industrial Security

That security is not a new issue to industry is self evident. An example is the American Society for Industrial Security (ASIS International) which has been established way back in 1955. ASIS...
International, with presently over 33,000 members, is an international organisation for professionals responsible for security, including managers and directors of security. ASIS is dedicated to increasing the effectiveness and productivity of security practices by developing educational programs and materials that address broad security concerns as well as specific security topics.

ASIS also has a European branch of which over 2,500 security professionals are member.

Following 9/11 ASIS has developed a number of guidelines which assist organisations and security professionals to improve the security and sustainability of their operations. Amongst these guidelines are:

- Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery: A guideline outlining a series of interrelated processes and activities, including readiness, prevention, response, recovery / resumption, testing and training, and evaluation and maintenance, that will assist in creating, assessing, and sustaining a comprehensive plan for use in the event of a crisis that threatens the viability and continuity of an organisation.
- Chief Security Officer Guideline: A guideline that addresses the key responsibilities and accountabilities, skills and competencies, and qualifications for an organisation’s senior security executive.
- General Security Risk Assessment Guideline: A seven-step process that creates a methodology by which security risks at a specific location can be identified and communicated, along with appropriate solutions.

Furthermore, the following guidelines are under development:

- Employment Screening Guideline (formerly Conducting Investigations): A guideline to aid employers in understanding the proper procedures, documentation, and related legal compliance issues concerning screening, conducting background checks on, obtaining credit reports on, and otherwise doing due diligence matters on volunteers, applicants for employment, and current employees.
- Protecting Information Guideline: A guidelines to offer general protection advice (collection, storage, dissemination, and destruction) for an entity’s information assets, including proprietary, classified, and marketing materials, etc.
- Physical Security Measures Guideline (formerly Security Countermeasures): A guideline to assist in the selection of appropriate physical security measures including defining risk levels, implementing an integrated set of physical security measures, and devising policies and procedures related to security incidents, access control, monitoring systems, lighting, security personnel, audits and inspection, etc.
- Workplace Violence Prevention and Response Guideline: A guideline to offer useful ways to maintain a safe and secure work environment through such means as identifying, evaluating, and controlling potential hazards and conducting employee informational training.

13. Multinationals implementation of own standards on suppliers

An increasing number of multinationals like Philips, IBM, Microsoft, Exxon, DHL, Maersk etc. have been or are in the process of developing security management systems which are also
covering their supply chain security operations. They do so, not only as a response to the already implemented regulatory requirements like C-TPAT and the ISPS, but mainly to protect their corporation against brand damage and to reduce losses due to theft.

Some of these programs are well developed and the implementation throughout the, mostly very complex, global organisation is supported by a system of self assessment. All these programs are characterised by the fact that they are managed by an executive manager, reporting to company’s top management.

What all these business driven supply chain security programs have in common is that they serve a dual strategy. These corporations are not only seeking acceptance from the wide range of custom organisations as AEO or as being C-TPAT compliant. In reaching for this status and to protect their assets they also start building secure supply chains by only utilising secure supply chain service suppliers such as forwarders, transport companies, warehouses, distributors, agents, insurers etc.

Whereas they now rely on proven experience with and self declaration by these service suppliers an increasing tendency develops that these multinationals wants to obtain greater confidence in the security management systems of their suppliers and start auditing them.

This will lead to a considerable economic burden for the logistic sector since in the fine mashed logistic network this will result that service suppliers need to comply with different standards, set by different clients and will be subjected to as many audits as they have larger clients.

14. ISO Supply Chain Security Management System Standards

To avoid this undesirable effect for industry ISO has taken the initiative to develop standards for security management of the supply chain.

Technical Committee 8 (Ships and Maritime Technology), who has been developing an ISO Specification on Port Security (ISO-PAS 20858) proved to be the only TC within ISO which was considered to be qualified to develop transport security related standards. This TC has been tasked to develop two Publicly Available Specifications, i.e.:

- ISO-PAS 28001: Best Practices Custody in Supply Chain Security

ISO-PAS 28000 is a high level standard which defines generic requirements with which supply chain security management systems shall comply. It is fully conversant with the ISO 14.000 standard (Environmental Management Systems) which reflects the state of the art thinking about management systems in industry.

ISO-PAS 28000 very much serves to be a systematic umbrella over more functional security management requirements such as defined in C-TPAT, StairSec®, WCO, ISPS, TAPA, ISO-PAS 28001 and the measures as defined in chapter 4 of this report.

Comparing the requirements in all these regulations and standards it is notable that they all are very similar and are addressing the same issues, using different wording and different degrees of detail.
ISO normally chooses the route to first develop a Publicly Available Standard where industry has the needs to have a standard available in short time. The formal approval process within the ISO system on PAS documents is relatively simple. If the need for a PAS is sustained after 2 years it will be developed into a Draft ISO Standard which then, through far more complex and comprehensive consultation process are developed into formal ISO standards.

Where the PAS 28.000 documents are expected to be available for industry by the end of 2005 the development of these documents into final ISO standards may take 4 to 6 years.

A working draft for PAS 28000 has been developed and will be circulated to the voting standardisation organisations by mid 2005.

A working draft for the PAS 28001 is under development and is expected to be ready for hearing by the voting standardisation organisations by September 2005.

In spite of the simplified voting procedure especially members of the working groups, developing the two PAS documents, representing organisations like Lloyds Register, Germanische Lloyd and Det Norske Veritas are determined that during the hearing process through the voting standards organisations all relevant trade and industry organisations are consulted to ensure sufficient bearing ground and industry acceptance.

Besides it will be ensured that the requirements, as defined in 28001 will be matching the measures as defined in chapter 4 of this report to ensure that possible future EU legislations in the area of supply chain security is able to make reference to ISO Standards.
Report Appendix D: Cost of security measures
### Specific Supply Chain Security Requirements Rail Repair Yards

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY MANAGEMENT SYSTEM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>0,5</td>
<td>2</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>0,1</td>
<td>0,2</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records ( Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

### General Security Requirements

#### Procedural security - General
- Implement procedures how deviations and anomalies are handled | 0,1 | 0,2 | 0 | 0 |
- Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled | 0,5 | 1 | 0 | 0 |
### Specific Supply Chain Security Requirements Rail Repair Yards

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies</td>
<td>Micro Enterprise &lt; 10 empl.</td>
<td>Small Enterprise &lt; 50 empl.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organization and within the supply chain are performed.</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>0,1</td>
<td>0,2</td>
</tr>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills</td>
<td>0,3</td>
<td>0,6</td>
</tr>
</tbody>
</table>

#### Human Resource Security - General

Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0,1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# Specific Supply Chain Security Requirements Rail Repair Yards

## Description of Requirement

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that security critical staff including sub-contracted staff, are screened and interviewed prior to employment and at reasonable intervals.</td>
<td>0,2 0,4 0,4 1</td>
<td></td>
</tr>
<tr>
<td>All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>1 2</td>
<td></td>
</tr>
</tbody>
</table>

## Specific Requirements to maintenance/repair organisations

### Procedural security to maintenance/repair organisations

| Ensure inspection of confined spaces of the rolling stock before (redelivery) | 0,1 0,1 | 3 8 |
| Ensure adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions. | 0,1 0,2 3 10 |

### Physical security to maintenance/repair organisations

| Ensure buildings containing critical working areas are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons and goods. | 5 12 0 0 |
| Ensure that critical working areas, situated outside, are surrounded by perimeter fences which comply to the legal and statutory requirements. | 22 36 0 0 |
| Ensure that critical working areas are fitted with doors, windows, gates and fences, provided with adequate locking devices. | 1 3 0 0 |
### Specific Supply Chain Security Requirements Rail Repair Yards

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that critical working areas, both inside and outside, as well as parking areas are provided with adequate lighting</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that critical working areas are equipped with intrusion alarms or its equivalent and that alarms are subject to 24 hour response and real time monitoring</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Ensure that parking areas for private vehicles are well separated from critical working areas</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that critical working areas, where appropriate, are patrolled by guards, dogs and/or closed TV-circuits.</td>
<td>8</td>
<td>0</td>
</tr>
</tbody>
</table>

**Access Controls to maintenance/repair organisations**

| Ensure that only authorized staff has access to critical working areas. Controls shall include positive identification and recording of all arriving and leaving employees, suppliers, visitors, vendors and incoming vehicles and their drivers. | 5 | 13 |
| Ensure that visitors are not moving around the facilities without accompaniment of a trusted employee | 0,1 | 1 |
| Ensure that unauthorized / unidentified persons are stopped and questioned | 0,1 | 1 |
| Ensure that restricted areas are clearly marked as such and unauthorized access to these areas is prevented or raises an alarm. | 3 | 0 |

- CONFIDENTIAL -

Reference to part of this report which may lead to misinterpretation is not permissible
### Specific Supply Chain Security Requirements Rail Repair Yards

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that authorization to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.</td>
<td>0,1</td>
<td>0,2</td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.</td>
<td>0,1</td>
<td>0,2</td>
</tr>
</tbody>
</table>

**MEASUREMENT, ANALYSES AND IMPROVEMENT**

**General**

The organization shall plan and perform internal audits and follow-up possible improvements needed. | 1 | 3 | 0,6 | 1 |

The organisation shall be audited by an authorised external 3rd party | 1 | 3 | 0,6 | 1 |

**TOTAL COST** | 63,4 | 138,9 | 30,8 | 87,8 |
### Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply one's mind to anti terrorist security.</td>
<td>0,1</td>
<td>0,5</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>0,1</td>
<td>0,5</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records (Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>0,1</td>
<td>0,5</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#### SECURITY MANAGEMENT SYSTEM

##### General system requirements
### Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled.</td>
<td>0 0,5 1 3</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies.</td>
<td>0 1 2 8</td>
<td>0 0,2 0,4 1</td>
</tr>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organization and within the supply chain are performed.</td>
<td>0 0 0 0</td>
<td>0,1 0,3 0,5 1,2</td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation.</td>
<td>0,1 1 3 8</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>0 0,1 0,2 0,3</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills.</td>
<td>0,1 0,3 0,6 1,5</td>
<td>0 1,5 3 6</td>
</tr>
</tbody>
</table>

**Human Resource Security - General**
### Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that security critical staff including subcontracted staff, are screened and interviewed prior to employment and at reasonable intervals.</td>
<td>0,1</td>
<td>0,2</td>
</tr>
<tr>
<td>All present and new employees, including subcontracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>0,1</td>
<td>0,5</td>
</tr>
</tbody>
</table>

### Specific Requirements to Transporters

#### Procedural security - transporters

| Ensure that only cargo is accepted to be loaded on the organization's means of conveyance which are properly marked, have the correct weight and documentation, and that the marking of the cargo (unit) and its seals are in accordance with the documentation. | 0                           | 0,1                       | 0,2                         | 0,3                         | 0,1                         | 0,5                       | 2                           | 4                           |
| Ensure that cargo units, whether stuffed-up or empty, only will be loaded when they are properly sealed and this sealing is properly recorded. | 0                           | 0,1                       | 0,2                         | 0,3                         | 0,1                         | 0,5                       | 2                           | 4                           |
### Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro Enterprise</td>
<td>Small Enterprise</td>
</tr>
<tr>
<td>Ensure that cargo is moved according to predefined schedules, including routes and stops, and unexpected delays and deviations are reported to the organization</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that security pertinent equipment is properly maintained and calibrated</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that before loading, at departure and after each prolonged stop, seals are checked for tampering, all readily accessible areas are physical searched and internal/external compartments and panels and other potential places of concealment of illegal or illicit goods are secured and/or inspected. These checks are to be recorded and records are to be kept for three months and be accessible to other actors in the supply chain for verification.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure rerouting of dangerous cargo to avoid routine patterns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that no unauthorised passengers are allowed on board.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that confined spaces are inspected after delivery or at redelivery after maintenance or repair.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

### physical security - freight transporters
### Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that control cabins of means of conveyance, when not manned, are kept locked at all times and only employees of the organization are allowed to have access.</td>
<td>0 0,1 0,2 0,3 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that keys are kept under control of the driver/operator at all times.</td>
<td>0 0,1 0,2 0,3 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that documentation containing cargo information is kept secure in these control cabins.</td>
<td>0 0,1 0,2 0,3 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that control cabins are equipped with an intrusion alarm.</td>
<td>1 4 30 100 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that other internal or external compartments or panels are kept locked when not under surveillance.</td>
<td>0 0,1 0,2 0,3 1 3,5 13 50</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that procedures are in place for reporting when unauthorized persons, unmanifested materials, or signs of tampering, are discovered.</td>
<td>0 0,1 0,2 0,3 0 2 6 20</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>Ensure that no prolonged stops are made at isolated locations where normal social control can not be exercised, unless such location is equipped with adequate lightening (and fencing) according to the standards set by the designated authorities.</td>
<td>0 0,1 0,2 0,3 1 3,5 13 50</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>
## Specific Supply Chain Security Requirements Transporters

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that vessels and barges are kept under constant surveillance, whether en route or boarded alongside and have adequate lightening etc. to prevent intrusion</td>
<td>0,1</td>
<td>0,3</td>
<td>0,2</td>
<td>0,5</td>
<td>0,1</td>
<td>0,3</td>
<td>0,2</td>
<td>0,5</td>
</tr>
<tr>
<td>Ensure that control rooms of traffic control centers are kept locked for non-authorised persons.</td>
<td>0,15</td>
<td>6</td>
<td>0,15</td>
<td>5,8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### MEASUREMENT, ANALYSES AND IMPROVEMENT

#### General
- The organization shall plan and perform internal audits and follow-up possible improvements needed.  
  - Implementation Cost (1000€): 0,5 1 3 5 0,2 1 1 2
- The organisation shall be audited by an authorised external 3rd party  
  - Implementation Cost (1000€): 0,5 1 3 5 0,2 1 1 2

### TOTAL COST
<table>
<thead>
<tr>
<th></th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2,7</td>
<td>12,4</td>
</tr>
<tr>
<td></td>
<td>48,95</td>
<td>147,5</td>
</tr>
<tr>
<td></td>
<td>3,75</td>
<td>19,4</td>
</tr>
<tr>
<td></td>
<td>58,65</td>
<td>202,5</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Warehouses

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>0,05</td>
<td>0,5</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records ( Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### General Security Requirements

**Procedural security - General**

- Implement procedures how deviations and anomalies are handled
  - Micro Enterprise: 0
  - Small Enterprise: 0,1
  - Medium Enterprise: 0,2
  - Large Enterprise: 0,3

- Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled.
  - Micro Enterprise: 0
  - Small Enterprise: 0,5
  - Medium Enterprise: 1
  - Large Enterprise: 2
### Specific Supply Chain Security Requirements Warehouses

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organization and within the supply chain are performed.</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills</td>
<td>0,1</td>
<td>0,3</td>
</tr>
</tbody>
</table>

### Human Resource Security - General

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that security critical staff including sub-contracted staff, are screened and interviewed prior to employment and at reasonable intervals.</td>
<td>0,1</td>
<td>0,2</td>
</tr>
</tbody>
</table>
## Specific Supply Chain Security Requirements: Warehouses

### Description of Requirement

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>0,1</td>
<td>0,4</td>
<td>3</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Specific Requirements to Warehouses, Storage Areas and Terminals

#### Procedural Security - warehouses

- **Ensure that all cargo entering the warehouse or storage area is properly marked, weighed, counted, documented and where appropriate inspected for the absence of illegal goods or attributes.**
  - Cost: 0.1, 1, 2, 4

- **Check that all cargo entering the premises are properly sealed and that the seal or alternative access monitoring devices and where possible the cargo is compliant to its documentation.**
  - Cost: 0, 0.1, 0.2, 0.3, 0.2, 1, 5, 10

- **Ensure the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading and check pre-alert information from origin sites. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers.**
  - Cost: 0, 0.1, 0.2, 0.3, 0.1, 1, 8, 16

- **Ensure that emptied cargo units are sealed again, with proper recording of such seals, or otherwise are secured against unauthorized access.**
  - Cost: 0, 0.1, 0.2, 0.3, 0.2, 0.4, 0.8, 1.6

---

Digital version of the table: [Download](#)
### Specific Supply Chain Security Requirements

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions</td>
<td>0</td>
<td>0.1</td>
</tr>
<tr>
<td>Ensure that an analysis is made of the vulnerability of information systems, the relevance to security of data and the implementation of adequate safeguards and firewalls.</td>
<td>0.1</td>
<td>4</td>
</tr>
<tr>
<td>Ensure that files and records are not removed from the office without permission.</td>
<td>0</td>
<td>0.1</td>
</tr>
<tr>
<td>Ensure that all computer users acknowledge receipt of, and consent to, the IT security policy as a condition of access to company systems.</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Ensure that all IT personnel with access to digital information, including those with indirect access by means of administrative privilege, receive training on information security principles. For certain personnel, this may include training on proper incident handling procedures.</td>
<td>0.1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that complete, legible and accurate documents, either electronically or conventionally, are submitted timely to designated authorities, in the format, means and at the time requested by them.</td>
<td>0</td>
<td>0.1</td>
</tr>
</tbody>
</table>
Specific Supply Chain Security Requirements Warehouses

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ensure that security critical information is securely stored, only accessible to authorized personnel and that the users of this information can be traced back</strong></td>
<td>0,1 4 8 16</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td><strong>Ensure that the security officer regularly checks information access logs to identify any unusual or out-of-hours activity.</strong></td>
<td>0 0 0 0</td>
<td>0 2 4 8</td>
</tr>
<tr>
<td><strong>Ensure that routines exist to securely cope with break downs and secure back-up routines are followed.</strong></td>
<td>0,1 0,1 0,2 0,3</td>
<td>0,1 2 8 16</td>
</tr>
<tr>
<td><strong>Ensure that the transporter is informed when during the processing of information it is noted that the progress or movement of CTU’s deviates from pre-defined schedules</strong></td>
<td>0 0,1 0,2 0,3</td>
<td>0 1 5 15</td>
</tr>
<tr>
<td><strong>Ensure that overages and shortages, as well as other anomalies, observed during the processing of information, are reported not only to the designated authorities, but also to the organization(s) responsible for the processing of the cargo.</strong></td>
<td>0 0,1 0,2 0,3</td>
<td>0 1 5 15</td>
</tr>
<tr>
<td><strong>Physical Security - warehouses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ensure that warehouses are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons and goods.</strong></td>
<td>0,3 2 8 20</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td><strong>Ensure that storage areas and terminals are surrounded by perimeter fences which comply to the legal and statutory requirements</strong></td>
<td>0,3 2 8 20</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>DESCRIPTION OF REQUIREMENT</td>
<td>Implementation Cost (1000€)</td>
<td>Maintenance Cost (1000€)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Ensure that critical working areas are fitted with doors, windows, gates and fences, provided with adequate locking devices.</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Ensure that critical working areas, both inside and outside, as well as parking areas are provided with adequate lighting</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that international-, domestic-, high-value- and dangerous goods cargo is marked and segregated within the premises by a safe, caged or otherwise fenced-in area.</td>
<td>0,1</td>
<td>4</td>
</tr>
<tr>
<td>Ensure that critical working areas are equipped with intrusion alarms or its equivalent and that alarms are subject to 24 hour response and real time monitoring</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Ensure that parking areas for private vehicles are well separated from critical working areas</td>
<td>0,1</td>
<td>3</td>
</tr>
<tr>
<td><strong>Access controls - warehouses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only authorized staff has access to critical working areas. Controls shall include positive identification and recording of all arriving and leaving employees, suppliers, visitors, vendors and incoming vehicles and their drivers.</td>
<td>0,15</td>
<td>7</td>
</tr>
<tr>
<td>Ensure that visitors are not moving around the facilities without accompaniment of a trusted employee</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

- CONFIDENTIAL -

Reference to part of this report which may lead to misinterpretation is not permissible

MANAGING RISK
<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that unauthorized / unidentified persons are stopped and questioned</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that restricted areas are clearly marked as such and unauthorized access to these areas is prevented or raises an alarm.</td>
<td>0,15</td>
<td>4</td>
</tr>
<tr>
<td>Ensure that authorization to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

Specific requirements to information processors, like forwarders etc.

**MEASUREMENT, ANALYSES AND IMPROVEMENT**

**GENERAL**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization shall plan and perform internal audits and follow-up possible improvements needed.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0,5</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>The organisation shall be audited by an authorised external 3rd party</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0,5</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>TOTAL COST</strong></td>
<td>5,45</td>
<td>56,1</td>
<td>129,4</td>
<td>269,5</td>
<td>3,15</td>
<td>38,1</td>
<td>132,5</td>
<td>260,5</td>
</tr>
</tbody>
</table>
## Specific Supply Chain Security Requirements Forwarders, Agents etc.

### Description of Requirement

<table>
<thead>
<tr>
<th>SECURITY MANAGEMENT SYSTEM</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>0.05 0.5 1 3 0 0.2 1 2</td>
<td></td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>0.1 1 3 9 0 0.2 0.5 1</td>
<td></td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>0 0.1 0.2 0.3 0 0.1 0.2 0.4</td>
<td></td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records ( Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>0.1 1 2 4 0.1 0.4 0.8 2</td>
<td></td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>0 0 0.1 0.1 0 0.1 0.2 0.4</td>
<td></td>
</tr>
</tbody>
</table>

### General Security Requirements

#### Procedural security - General

Implement procedures how deviations and anomalies are handled | 0 0.1 0.2 0.3 0 0 0 0 |
## Specific Supply Chain Security Requirements Forwarders, Agents etc.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled.</td>
<td>0</td>
<td>0,5</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>0,1</td>
<td>0,3</td>
<td>1</td>
</tr>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organization and within the supply chain are performed.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0,1</td>
<td>0,3</td>
<td>0,6</td>
<td>1,2</td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td>0,1</td>
<td>1,5</td>
<td>3</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>0</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills</td>
<td>0,1</td>
<td>0,3</td>
<td>0,6</td>
<td>1,5</td>
<td>0</td>
<td>0,8</td>
<td>1,5</td>
<td>3</td>
</tr>
</tbody>
</table>

### Human Resource Security - General
### Specific Supply Chain Security Requirements Forwards, Agents etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that security critical staff including sub-contracted staff, are screened and interviewed prior to employment and at reasonable intervals.</td>
<td>0.1</td>
<td>0.2</td>
</tr>
<tr>
<td>All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>0.1</td>
<td>0.5</td>
</tr>
</tbody>
</table>

### Specific requirements to information processors, like forwards etc.

#### Procedural security - information processors, like forwards etc.

| Ensure that an analysis is made of the vulnerability of information systems, the relevance to security of data and the implementation of adequate safeguards and firewalls. | 0.1 | 3 | 7 | 15 | 0 | 0 | 0 | 0 |
| Ensure that files and records are not removed from the office without permission. | 0 | 0.1 | 0.2 | 0.3 | 0 | 0 | 0 | 0 |
| Ensure that all computer users acknowledge receipt of, and consent to, the IT security policy as a condition of access to company systems. | 0.1 | 0.1 | 0.2 | 0.3 | 0 | 0.1 | 0.5 | 2.5 |
### Specific Supply Chain Security Requirements Forwarders, Agents etc.

#### DESCRIPTION OF REQUIREMENT

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all IT personnel with access to digital information, including those with indirect access by means of administrative privilege, receive training on information security principles. For certain personnel, this may include training on proper incident handling procedures.</td>
<td>0,1 2 5 15 0,05 1 3 8</td>
<td></td>
</tr>
<tr>
<td>Ensure that complete, legible and accurate documents, either electronically or conventionally, are submitted timely to designated authorities, in the format, means and at the time requested by them.</td>
<td>0 0,1 0,2 0,3 0 0 0 0</td>
<td></td>
</tr>
<tr>
<td>Ensure that security critical information is securely stored, only accessible to authorized personnel and that the users of this information can be traced back</td>
<td>0,1 4 8 16 0 0 0 0</td>
<td></td>
</tr>
<tr>
<td>Ensure that the security officer regularly checks information access logs to identify any unusual or out-of-hours activity.</td>
<td>0 0 0 0 0 0,8 1,5 3</td>
<td></td>
</tr>
<tr>
<td>Ensure that routines exist to securely cope with breakdowns and secure back-up routines are followed.</td>
<td>0,1 0,1 0,2 0,3 0,1 1,5 5 12</td>
<td></td>
</tr>
<tr>
<td>Ensure that the transporter is informed when during the processing of information it is noted that the progress or movement of CTU’s deviates from pre-defined schedules</td>
<td>0 0,1 0,2 0,3 0 1 4 10</td>
<td></td>
</tr>
</tbody>
</table>

- CONFIDENTIAL -

Reference to part of this report which may lead to misinterpretation is not permissible

MANAGING RISK
### Specific Supply Chain Security Requirements Forwarders, Agents etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that overages and shortages, as well as other anomalies, observed during the processing of information, are reported not only to the designated authorities, but also to the organization(s) responsible for the processing of the cargo.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

**Physical Security - Information Processors, like forwarders etc.**

| Ensure that buildings containing critical working areas are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons. | 0 | 0,1 | 0,2 | 0,3 | 0 | 0 | 0 | 0 |
| Ensure that external and internal doors and windows of critical working areas are provided with locking devices and maintained to perform their designate functions. | 0 | 0,1 | 0,2 | 0,3 | 0 | 0 | 0 | 0 |
| Ensure that critical working areas are equipped with intrusion alarms or its equivalent | 0 | 0,1 | 0,2 | 0,3 | 0 | 0 | 0 | 0 |

**Access Controls - Information Processors, like forwarders etc.**

| Ensure that critical working areas are clearly marked as such and unauthorized access to these areas is prevented or raises an alarm. | 0 | 0,1 | 0,2 | 0,3 | 0 | 0 | 0 | 0 |
| Ensure that controls include positive identification and recording of all employees, suppliers, visitors, and vendors in the premises. | 0 | 0,1 | 0,2 | 0,3 | 0,1 | 0,8 | 5 | 10 |
### Specific Supply Chain Security Requirements Forwarders, Agents etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that visitors are not allowed to move around the facilities without accompaniment of an employee</td>
<td>0 0,1 0,2 0,3 0,2 0,8 5 10</td>
<td>0 0,1 0,2 0,3 0 0,2 1 3</td>
</tr>
<tr>
<td>Ensure that unauthorized / unidentified persons are stopped and questioned</td>
<td>0 0,1 0,2 0,3 0 0,5 3 6</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
</tr>
<tr>
<td>Ensure that authorization to access critical working areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
<td>0 0,1 0,2 0,3 0,1 0,2 0,4 0,8</td>
</tr>
</tbody>
</table>

### MEASUREMENT, ANALYSES AND IMPROVEMENT

<table>
<thead>
<tr>
<th>General</th>
<th>0,5 1 3 5 0,2 1 1 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization shall plan and perform internal audits and follow-up possible improvements needed.</td>
<td>0,5 1 3 5 0,2 1 1 2</td>
</tr>
<tr>
<td>The organisation shall be audited by an authorised external 3rd party</td>
<td>0,5 1 3 5 0,2 1 1 2</td>
</tr>
</tbody>
</table>

### TOTAL COST

<p>|  | 2,05 18,9 43 96,4 1,45 13,2 42,9 102,1 |</p>
<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th></th>
<th></th>
<th>Maintenace Cost (1000€)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Micro Enterprise</td>
<td>Small Enterprise</td>
<td>Medium Enterprise</td>
<td>Large Enterprise</td>
<td>Micro Enterprise</td>
<td>Small Enterprise</td>
</tr>
<tr>
<td></td>
<td>&lt; 10 empl.</td>
<td>&lt; 50 empl.</td>
<td>&lt; 250 empl.</td>
<td>&gt; 250 empl.</td>
<td>&lt; 10 empl.</td>
<td>&lt; 50 empl.</td>
</tr>
<tr>
<td>Security Management System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General system requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make an assessment of terrorist risks and mitigation measures already in place and apply ones mind to anti terrorist security.</td>
<td>0,05</td>
<td>0,5</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0,3</td>
</tr>
<tr>
<td>Document measures/procedures in a security manual</td>
<td>0,1</td>
<td>0,5</td>
<td>3</td>
<td>7</td>
<td>0</td>
<td>0,3</td>
</tr>
<tr>
<td>Implement document control procedures to ensure that only valid documents are accessible to those who need them and are allowed access to these documents</td>
<td>0</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Implement procedures to maintain security relevant records ( Legislative and regulatory requirements, Cargo manifests, Permits, Initial and periodic employee screening records, instructions on contact with authorities etc.)</td>
<td>0,1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>0,1</td>
<td>0,5</td>
</tr>
<tr>
<td>Appointed a member of management who, irrespective of other responsibilities, has responsibility and authority to implement the security management system.</td>
<td>0</td>
<td>0</td>
<td>0,2</td>
<td>0,2</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>General Security Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedural security - General</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement procedures how deviations and anomalies are handled</td>
<td>0</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- CONFIDENTIAL -
Reference to part of this report which may lead to misinterpretation is not permissible
MANAGING RISK
# Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement procedures how seals shall be attached, inspected, recorded, stored or otherwise be handled,</td>
<td>0</td>
<td>0,5</td>
</tr>
<tr>
<td>Ensure that only suppliers/subcontractors are used which have a confirmed secure operation and avoid the use of bogus companies</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Ensure that random, unannounced security verification of areas in control of the organization and within the supply chain are performed.</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Implement procedures how to prepare emergency or last-minute shipments and how designated authorities shall be notified.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

#### DESCRIPTION OF REQUIREMENT

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe how the response will be to any security threat and breaches, including information to authorities, emergency planning, crisis management, emergency and evacuation procedures, training and drills</td>
<td>0,1</td>
<td>0,3</td>
<td>0,6</td>
<td>1,5</td>
<td>0</td>
<td>1,5</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

#### Human Resource Security - General

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define which positions in the organisation are security critical and ensure that authorities, roles and responsibilities are clearly defined for both internal and external security relevant persons</td>
<td>0</td>
<td>0</td>
<td>0,1</td>
<td>0,3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure that security critical staff, including sub-contracted staff, are screened and interviewed prior to employment and at reasonable intervals.</td>
<td>0,1</td>
<td>0,2</td>
<td>0,4</td>
<td>0,8</td>
<td>0,1</td>
<td>0,4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>All present and new employees, including sub-contracted staff, shall be periodically made aware of security risks and receive relevant training</td>
<td>0,1</td>
<td>0,6</td>
<td>3</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

#### DESCRIPTION OF REQUIREMENT

<table>
<thead>
<tr>
<th>Description</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that a trusted employee is physically present during loading/unloading of the cargo unit to supervise the introduction or removal of cargo to prevent that the physical security of the cargo is inflicted. This supervision shall be uninterrupted from the start of the inspection until the cargo is sealed</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that this trusted employee at closing of the cargo unit is providing it with a seal and record relevant details in compliance with the companies sealing procedure</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ensure verification that seals on received cargo are intact and conform the appropriate records.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that empty or partially loaded cargo units are inspected to detect any security breach or compromising of the integrity of the unit immediately before loading</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that all cargo is compliant with its documentation and manifests</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all cargo entering the warehouse or storage area is properly marked, weighed, counted, documented and where appropriate inspected for the absence of illegal goods or attributes.</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Ensure the identity and authority of carriers, requesting delivery or collection of cargo is verified before discharge/loading and check pre-alert information from origin sites. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that any units partly packed at end of business is securely locked to restrict access.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that seals are stored under controlled conditions, not be used in numeric sequence and that records on seals are verified by a second person</td>
<td>0,2</td>
<td>0,4</td>
</tr>
<tr>
<td>Perform adequate periodic inspection, maintenance, repair and calibration to ensure the integrity of security pertinent equipment or provisions.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that only containers, swap bodies, trailers etc are used which are acceptable to the regulatory authorities.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>

- Most of this should be normal practice already
- Combine partly with access control

MANAGING RISK

Reference to part of this report which may lead to misinterpretation is not permissible
## Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that an analysis is made of the vulnerability of information systems, the relevance to security of data and the implementation of adequate safeguards and firewalls.</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that files and records are not removed from the office without permission.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that all computer users acknowledge receipt of, and consent to, the IT security policy as a condition of access to company systems.</td>
<td>0,1</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that all IT personnel with access to digital information, including those with indirect access by means of administrative privilege, receive training on information security principles. For certain personnel, this may include training on proper incident handling procedures.</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that complete, legible and accurate documents, either electronically or conventionally, are submitted timely to designated authorities, in the format, means and at the time requested by them.</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>
## Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

**DESCRIPTION OF REQUIREMENT**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ensure that security critical information is securely stored, only accessible to authorized personnel and that the users of this information can be traced back</strong></td>
<td>0,1</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td><strong>Ensure that the security officer regularly checks information access logs to identify any unusual or out-of-hours activity.</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Ensure that routines exist to securely cope with break downs and secure back-up routines are followed.</strong></td>
<td>0,1</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
</tr>
<tr>
<td><strong>Ensure that the transporter is informed when during the processing of information it is noted that the progress or movement of CTU’s deviates from pre-defined schedules</strong></td>
<td>0</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
</tr>
<tr>
<td><strong>Ensure that overages and shortages, as well as other anomalies, observed during the processing of information, are reported not only to the designated authorities, but also to the organization(s) responsible for the processing of the cargo.</strong></td>
<td>0</td>
<td>0,1</td>
<td>0,2</td>
<td>0,3</td>
</tr>
</tbody>
</table>

**Physical security - Shippers**

*CONFIDENTIAL*

Reference to part of this report which may lead to misinterpretation is not permissible

MANAGING RISK
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that critical areas for production, storage and administration are constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons and goods.</td>
<td>0,8</td>
<td>5</td>
</tr>
<tr>
<td>Ensure that these critical areas are surrounded by perimeter fences which comply to the legal and statutory requirements</td>
<td>0,8</td>
<td>5</td>
</tr>
<tr>
<td>Ensure that these critical working areas are fitted with doors, windows, gates and fences, provided with adequate locking devices.</td>
<td>0,1</td>
<td>1</td>
</tr>
<tr>
<td>Ensure that critical working areas, both inside and outside, as well as parking areas are provided with adequate lighting</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that critical working areas are equipped with intrusion alarms or its equivalent and that alarms are subject to 24 hour response and real time monitoring</td>
<td>0,6</td>
<td>4</td>
</tr>
<tr>
<td>Ensure that parking areas for private vehicles are well separated from critical working areas</td>
<td>0,1</td>
<td>2</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

<table>
<thead>
<tr>
<th>DESCRIPTION OF REQUIREMENT</th>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that international-, domestic-, high-value- and dangerous goods cargo is marked and segregated within the premises by a safe, caged or otherwise fenced-in area.</td>
<td>0,1</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that all loading and discharge valves and inspection hatches of dangerous cargo transports are provided with (pad)locks</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that dry-bulk cargo is covered by tarpaulins or hatches, which are properly sealed.</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that critical working areas, where appropriate, are patrolled by guards, dogs and/or closed TV-circuits.</td>
<td>0,1</td>
<td>8</td>
</tr>
<tr>
<td>Access Controls - Shippers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure that only authorized staff has access to critical working areas. Controls shall include positive identification and recording of all arriving and leaving employees, suppliers, visitors, vendors and incoming vehicles and their drivers.</td>
<td>0,2</td>
<td>5</td>
</tr>
<tr>
<td>Ensure that visitors are not moving around the facilities without accompaniment of a trusted employee</td>
<td>0</td>
<td>0,1</td>
</tr>
<tr>
<td>Ensure that unauthorized / unidentified persons are stopped and questioned</td>
<td>0</td>
<td>0,1</td>
</tr>
</tbody>
</table>
### Specific Supply Chain Security Requirements Shippers, Manufacturers etc.

#### DESCRIPTION OF REQUIREMENT

<table>
<thead>
<tr>
<th>Implementation Cost (1000€)</th>
<th>Maintenance Cost (1000€)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Micro Enterprise</strong></td>
<td><strong>Small Enterprise</strong></td>
</tr>
<tr>
<td>&lt; 10 empl.</td>
<td>&lt; 50 empl.</td>
</tr>
<tr>
<td>Ensure that restricted areas are clearly marked as such and unauthorized access to these areas is prevented or raises an alarm.</td>
<td>0,2 3 6 12</td>
</tr>
<tr>
<td>Ensure that authorization to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times</td>
<td>0 2 4 6</td>
</tr>
<tr>
<td>Ensure that security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.</td>
<td>0 0,1 0,2 0,3</td>
</tr>
<tr>
<td>Ensure that upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall</td>
<td>0 0,1 0,2 0,3</td>
</tr>
</tbody>
</table>

#### MEASUREMENT, ANALYSES AND IMPROVEMENT

**General**

The organization shall plan and perform internal audits and follow-up possible improvements needed. | 0,5 1 3 5 | 0,2 0,6 1 2 | |

The organisation shall be audited by an authorised external 3rd party | 0,5 1 3 5 | 0,2 0,6 1 2 | |

**TOTAL COST** | 5,45 55,7 139,5 305,9 | 2,7 43,4 135,9 307,8 |
Report Appendix E: TAPA requirements
Contents

Section 1 - Requirements

1. Scope
   (a) Forward
   (b) Freight Security Requirements
   (c) Other Documents Referenced to FSR
   (d) FSR Applicable Areas
   (e) Resources to Implement the FSR
   (f) Definitions

2. Contract Acceptance
   (a) Suppliers' Responsibilities at Acceptance of the Contract

3. Supplier Security Organization
   (a) Supplier Security Representative
   (b) Supplier Loss Investigator

4. Risk Assessment and Audits
   (a) Buyers and Suppliers Responsibilities for Risk Assessments and Audits
   (b) Monitoring Supplier Corrective Action Requirements
   (c) Storage/Warehousing Building Classification Assessment
   (d) Supplier/Buyer Facility Security Audit Schedule

5. Security/Loss Investigations
   (a) Supplier Investigation Responsibilities

6. Waivers
   (a) Waivers
   (b) Waiver Process

7. Supplier Facility and Truck Security
   (a) Procedures
   (b) Supplier Facility Security Requirements (Summary)
   (c) Handling Operations
   (d) High Value Shipments by Truck (Summary)
Section 2 – Specifications  
1. Supplier Facility/Truck Freight Security Requirements

Section 3 – Forms  
FORM 3.1 – REQUEST FOR WAIVER

Section 1 - Requirements

1. Scope

(a) Forward

Technology Asset Protection Association (TAPA) is an association of security professionals and related business partners from high technology and high value companies who have organized for the purpose of addressing the emerging security threats that are common to the high value industry supply chain. A fundamental TAPA objective is to affect positive change in the security practices of the freight transportation and insurance communities as a whole. Major freight service providers are moving toward TAPA-recognized security standards for the care and handling of freight, and are recognizing the inherent value of doing so.

(b) Freight Security Requirements

Freight Security Requirements (FSR) have been established to ensure the safe and secure in-transit storage and warehousing of any TAPA members (Buyers) assets throughout the world. The FSR specifies the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards. The FSR outlines the process and specification for Suppliers to attain TAPA certification for their facilities and transit operations. It is the intention of TAPA members to select Suppliers that meet or exceed TAPA certification requirements. The successful implementation of the FSR is dependent upon Suppliers, TAPA Certified Auditors and Buyer working in concert. However, the safe and secure in-transit storage and warehousing of the Buyers assets is the complete responsibility of the Supplier, its agents and sub-contractors, throughout the collection, transit and delivery to the recipient, as specified in a Release. The FSR will be referenced in any contract between the Supplier and Buyer, and into the Supplier’s own security program. Unless prior arrangements or agreements have been negotiated and documented between the Supplier and Buyer, failure to implement any part of the FSR shall be construed as a material breach of contract.
(c) Other Documents Referenced to FSR

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Revision date</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAPA Freight Assessment Users Guide</td>
<td>To provide detailed definition and assessment criteria for Buyer &amp; TAPA certified independent assessors. (Not available to Supplier)</td>
<td>Jan 1, 2005</td>
</tr>
<tr>
<td>TAPA Pre-Certification Review Planning</td>
<td>Details the process to plan and conduct the pre-certification meeting. This meeting will assist in determining if Supplier facilities &amp; transportation methods meet the minimum-security requirements. For use by Buyer &amp; TAPA certified independent assessors. (Not available to Supplier)</td>
<td>Jan 1, 2005</td>
</tr>
</tbody>
</table>

(d) FSR Applicable Areas

The FSR shall apply to all geographical areas, and all such services provided. In geographical areas where English is not the first language, where necessary and applicable it is the joint responsibility of the Buyer and Supplier to ensure that the translation accurately reflects the intentions of the Buyer and to ensure that every relevant employee has been trained to implement the FSR.

(e) Resources to Implement the FSR

The resources to meet the requirements of the FSR shall be the responsibility of the Supplier and at Supplier’s own expense, unless as negotiated by or otherwise agreed to by Buyer and Supplier.

(f) Definitions

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer</td>
<td>TAPA Member or authorized agent, example being the TAPA certified audit body</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>DVR / DVMR</td>
<td>Digital Video Recorder</td>
</tr>
<tr>
<td>FSR</td>
<td>Freight Security Requirements</td>
</tr>
<tr>
<td>Local crime</td>
<td>Criminal incidents occurring within a 5 mile radius of Supplier’s facilities or transportation routes.</td>
</tr>
<tr>
<td>RSP</td>
<td>Retail Sales Price</td>
</tr>
<tr>
<td>SCAR</td>
<td>Supplier Corrective Action Requirement</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>TAPA CA</td>
<td>Technology Asset Protection Association Certified Auditor</td>
</tr>
<tr>
<td>VCR</td>
<td>Video Cassette Recorder</td>
</tr>
</tbody>
</table>

2. **Contract Acceptance**

(a) **Suppliers' Responsibilities at Acceptance of the Contract**

At acceptance of the contract, the Supplier shall submit to the regional representatives of the Buyer’s Logistics organization and the Buyer’s Security Management, a copy of the Supplier’s security policy and procedures or plan for ensuring safe and secure transportation, in-transit storage and warehousing of Buyer’s assets. Copies of Supplier’s security procedures that are relevant to the security of Buyer’s assets shall be submitted to the Buyer for review. Supplier’s security procedures must not conflict with the agreed to FSR. Any and all documentation shall be handled as confidential information. In cases where the Supplier’s security procedures do not meet the FSR, the Supplier shall take the following actions:

I. The Supplier shall present a detailed written action plan, which outlines the non-compliant FSR area and the corrective action to be taken, with implementation dates not to exceed 60 days from date of acceptance of contract.

II. Supplier will attain TAPA Certification within 60 days for all facilities that will handle Buyers assets.

III. For areas that are not FSR compliant, a negotiated contingency plan between Supplier & Buyer shall be agreed and in place at commencement of contract. The contingency plan is designed for use where Supplier needs time to upgrade security on new routes and shall not exceed 60 days in duration.

IV. Any exception to the 60 day duration referenced herein shall have prior written approval from the Buyer requiring FSR certification.

V. Supplier will note and respond to Buyers concerns regarding security concerns not covered by the FSR.

VI. The Supplier will only negotiate with the approved TAPA Certification body for waivers for non-applicable TAPA FSR security measures or where alternative actions are taken to control security risks. The regional TAPA governing body will approve/decline all waivers submitted by the supplier through the independent audit firm.

VII. Suppliers who submit to FSR certification independent of a Buyer’s requirement are not exempt from any portion of the FSR.
3. Security Organization

(a) Supplier Security Representative

By the effective date of the contract, the Supplier will designate a representative to liaise with the Buyer’s representatives. The Supplier’s Security Representative shall:

I. Have the Supplier’s designated security authority responsible for managing the compliance with the FSR.

II. Have an adequate level of security competence and background.

III. Assign at least one individual, security responsibilities for each of the geographical areas in which the contract is effective.

(b) Supplier Loss Investigator

By the effective date of the contract, the Supplier will designate one or more Loss Investigators for leading and coordinating investigation and resolution of losses of Buyer’s assets while under the responsibility of the Supplier. The Supplier shall ensure adequate and timely resources are available to investigate losses of Buyers assets in the location the loss is suspected to have occurred. Loss Investigators may be the same person as the Suppliers Security Representative, as long as both responsibilities are covered in full.

4. Risk Assessment and Audits

(a) Buyers and Suppliers Responsibilities for Risk Assessments and Audits

I. At acceptance of a contract between the Buyer and the Supplier, the Supplier agrees to Buyer’s right to conduct risk assessments or audits of all transit, storage and warehousing locations that will be used for Buyer’s assets. Buyer can nominate an agent to perform audits on behalf of the Buyer. Normally the Buyer or its agent shall notify the Supplier at least five working days in advance of any audit, detailing its nature.

II. Supplier shall ensure the TAPA certified audit body is engaged to ensure FSR audits and certification process is completed. Costs for TAPA certification shall be the responsibility of the Supplier.

III. The requirement for TAPA certification is also extended to Supplier’s sub-contractor’s facilities and in-transit locations, where used to transit Buyer’s assets.

IV. The Buyer reserves the right to conduct unscheduled audits. The Buyer shall give a minimum of 24 hours notice to the Supplier.

V. TAPA certified auditors shall inform the Supplier of assessment/audit results within ten working days from the completion of the audit. A summary of the probable findings/results should be given informally to the Supplier on the day of the audit/assessment at the closing conference.
VI. Supplier shall have deemed to pass the audit and certified if a TAPA FSR audit score of 60% or more is achieved and all mandatory items are scored at least 1. Supplier shall still be responsible for completing audit action items in the agreed time scale, even when certification is achieved. Clearance of the non-mandatory SCAR is at the option of the Supplier but must be disclosed to Buyer.

VII. When the TAPA certified auditor submits a SCAR (Supplier Corrective Action Requirement) to the Supplier associated with the audit findings, the Supplier shall respond to the auditor within ten working days, documenting the action to be taken, the date the action will be completed. SCAR completion dates may be negotiated between the auditor and the Supplier. However, unless the TAPA certification body approves a waiver from process, corrective action implementation shall not exceed sixty days from notification to the Supplier.

VIII. The Supplier is required to complete self-audits of their facilities and their subcontractor’s facilities as detailed in section IV paragraph (d).

(b) Monitoring Supplier Corrective Action Requirements

The Supplier shall submit to the TAPA auditor progress updates on all outstanding SCAR’s at monthly intervals. Any SCAR’s not completed on or before the due date are to be escalated by the Supplier’s Security Representative to the Supplier’s Management and reasons for non-compliance are to documented and communicated to the TAPA auditor. Supplier failure to address SCAR’s may result in the TAPA certification being withdrawn or suspended. The Supplier has the right to appeal to TAPA directly if certification is withdrawn. TAPA will agree to a process for adjudication between the Supplier and the TAPA auditor and has the right to impose a resolution on both parties.

(c) Storage/Warehousing Building Classification Assessment

The Building Classification Assessment is designed to categorize the facility into one of three categories, “A” being the highest security requirement and “C” the lowest. For facilities not previously classified, the Supplier must complete a classification assessment before the effective date of the contract and give results to the Buyer. Separate TAPA audit forms for A, B, & C facilities exist. The Supplier, in cooperation with the TAPA auditor, shall complete the final classification assessment within 30 days of acceptance of contract. The TAPA Certification body shall periodically complete their own classification assessments and ultimately make the decision on the final classification to be assigned to each of Supplier facilities handling or storing of Buyer’s assets. The Supplier or Buyer can request the facility to be re-assessed if either party considers the assessment category to have changed.

I. The Building Classification Assessment methodology is set forth below.

- Pre-Contract & where TAPA Certification has not been previously granted.
  - Using TAPA audit forms Supplier classifies facilities that will be used in the transpiration of Buyers assets by being rated at least 1 in each of the mandatory audit areas and obtain a score 60% or greater on the audit score.
  - Final classification is attained (within 30 days), when the Supplier facility complies with or has agreements in place with the TAPA auditor, that will
meet all the requirements of a category and is assessed by an independent TAPA auditor.

### (d) Supplier/Buyer Facility Security Audit Schedule

For the duration of the contract the Supplier will conduct security audits of their or their subcontractor’s facility in line with the audit schedule published below. The format of the audit is to be agreed with the Buyer. It is suggested the Supplier use the same audit format as the Buyer will use in Section 3. Results of Supplier self-audits shall be forwarded to the certifying body within 2 weeks of the self-assessment. A self-assessment is to be conducted annually within the anniversary month of the independent audit.

Supplier will allow Buyer to conduct audits when pre-arranged. Supplier will as a minimum audit the Supplier’s facilities in line with the audit requirements published below. The Buyer or the TAPA Certified Auditor reserves the right to increase or decrease the frequency of the audits by giving prior notification to the Supplier. The format of the TAPA audits will be to use the standard audit format contained in Section 3.

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>SUPPLIERS/SUBCONTRACTORS</th>
<th>SECURITY AUDIT REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>“A”</td>
<td></td>
<td>• Independent auditor: Certification audit conducted 1st year, validation audit conducted the following year (Note: Certification audits are conducted every other year)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supplier Self Assessment: Annually and submitted to TAPA CA body within two weeks of original certification anniversary.</td>
</tr>
<tr>
<td>“B”</td>
<td></td>
<td>• Independent auditor: Certification audit conducted 1st year, validation audit conducted the following year (Note: Certification audits are conducted every other year)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supplier Self Assessment: Annually and submitted to TAPA CA body within two weeks of original certification anniversary.</td>
</tr>
<tr>
<td>“C”</td>
<td></td>
<td>• No audits by Buyer or independent auditor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supplier audits, when requested by Buyer</td>
</tr>
</tbody>
</table>

### 5. Security/Loss Investigations

#### (a) Supplier Investigation Responsibilities

1. The Supplier, its agents and sub-contractors shall actively cooperate with law enforcement authorities, and the Buyer or their appointed agents in the conduct of an investigation into product, material or equipment that is lost, stolen, damaged or tampered with while under the responsibility of the Supplier or when the Supplier can provide assistance to any such investigation. All information, including regular
6. Waivers

(a) Waivers

In exceptional circumstances, the TAPA CA may be confronted with a waiver request for a specific security requirement in part or whole on behalf of the supplier. TAPA has a sub team that reviews and approves/denies all waiver request. It is the TAPA CA's responsibility to decide whether the request is valid and that substantial mitigating reason(s) exist that led to the waiver application. Request for waivers are more likely to be approved by TAPA if alternative security controls are introduced to mitigate the security exposure. Waivers are valid for up to a maximum of 1 year. The original requirement must be completed on the expiration date of the waiver or requested and approved again.

Waiver Process

I. Supplier considers a specific requirement in the FSR is not required from a security standpoint.

II. Supplier completes and submits Request For Waiver form to TAPA CA (See Section 3). One form should be completed for each FSR waiver request

III. TAPA CA reviews waiver request(s) and determines if request is valid. Each TAPA region currently administers waiver requests independently and the regional Board of Directors should be contacted for appropriate waiver process.

IV. If approved:

- Waiver specifics are documented and signed by the TAPA Certified Auditor
- TAPA Certified Auditor assigns date for how long waiver will be approved, sends copy to Supplier
- Supplier will meet all requirements of waiver in agreed time scales. Failure to do so will result in waiver approval being removed.
- TAPA Certified Auditor informs Buyer of waiver.

V. If not approved:

- Supplier required to implement full requirement of FSR
7. Supplier Facility and Truck Security

(a) Procedures

Section 2 lists the detailed requirements for the Supplier’s security procedures.

(b) Supplier Facility Security Requirements (Summary)

The Supplier’s facility security is to be based on good physical barriers, the efficient operation of intruder alarm and CCTV surveillance and strict adherence to agreed operational procedures. The facility should not be located in an area that has a high incidence of crime or is adjacent to derelict land or a run-down area. Requirements for the Supplier’s facility physical security are detailed in Section 2.

For purposes of audit, Preventive Measures are specific tactics to achieve acceptable levels of security for a given Area of Concern as identified in the TAPA audit form. These specific tactics have been identified through the knowledge and experience of industry security and logistics professionals, and represent best known methods and proven operational processes. However, in evaluating specific Preventive Measures of an individual Supplier, where such Supplier employs alternative methods that result in meeting or exceeding security requirements of the FSR, such methods shall be accepted, and rationale for acceptance noted in the audit “Comments” section. Additionally, specific tactics in the audit form which are in direct violation of Supplier documented policies and procedures shall be considered for removal from audit scoring on a case-by-case basis.

(c) Handling Operations

The various points at which the Buyer’s assets will be transferred from one operation to another (i.e. truck to warehouse, warehouse to truck, truck to airline handler, airline handler to aircraft are all viewed as areas of risk. The Supplier shall ensure all procedures for these operations are detailed and communicated to the Buyer. The Supplier shall notify the Buyer of any known deviation from these procedures.

(d) High Value Shipments by truck (Summary)

Shipments of Buyer’s assets by truck between the Suppliers facilities and delivery to the final destination shall be subject to minimum-security requirements. The table in Section 2 also specifies the truck security requirements. The level of Security required is dependant on independent agreement between Buyer and Supplier.
Section 2 – Specifications

Contents:

1. Supplier Facility/Truck Freight Security Requirements

<table>
<thead>
<tr>
<th>Supplier Facility/Truck Freight Security Requirements</th>
<th>Applicable to Final Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓ M = Requirement &amp; mandatory to pass audit</td>
<td></td>
</tr>
</tbody>
</table>

1. Perimeter Security

1.2. CCTV Systems

1.2.1 CCTV external coverage of shipping and receiving yard, including entry / exit point, to cover movement of vehicles and people

1.2.2 CCTV coverage of all external dock area. (Refer to "Clarification Document")

1.2.3 CCTV system able to view all sides of the facility.

|                               | ✓ M | ✓ M | ✓ M |

1.3. Lighting

1.3.1 Flood lighting of enclosed loading/unloading areas

1.3.2 Dock doors illuminated externally at night

1.3.3 External and internal lighting levels that support high quality CCTV images and recording

1.4 Perimeter alarm detection

1.4.1 All facility external doors alarmed and linked to main alarm system.

|                               | ✓ M | ✓ M | ✓ M |

1.5 Perimeter windows, doors & other openings
### Supplier Facility/Truck Freight Security Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Applicable to Final Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ M = Requirement &amp; mandatory to pass audit</td>
<td>A</td>
</tr>
<tr>
<td>✓ 1.5.1 Any windows or other openings in warehouse walls/roof must be secured by steel bars/mesh (or any other material that would harden opening to burglary).</td>
<td>✓</td>
</tr>
<tr>
<td>✓ 1.5.2 Ground floor warehouse windows protected by anti-ram posts or other physical barrier. (If no windows, not applicable, mark “X” on audit form)</td>
<td>✓</td>
</tr>
<tr>
<td>✓ 1.5.3 Dock doors of sufficient strength or design to prevent or delay forced entry by use of portable hand tools or ramming by vehicle.</td>
<td>✓</td>
</tr>
<tr>
<td>✓ 1.5.4 Reinforced exit doors from warehouse (steel doors and frames or suitable alternative).</td>
<td>✓</td>
</tr>
<tr>
<td>✓ 1.5.5 Exterior walls to be designed to resist penetration by removing building fabric, cutting or ramming by vehicle</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 2. Access Control – Office Areas

#### 2.1 Office Entrances

- 2.1.1 Visitor office access points controlled. ✓

#### 2.1.2. All office access points controlled. ✓ M ✓ M

#### 2.1.3. Access control processes both during and outside normal operating hours to ensure access is granted only for authorized Supplier employees and visitors. ✓ ✓ ✓ M

### 3. Facility Dock/Warehouse

#### 3.1. Access control between office and dock/warehouse

- 3.1.1 Security controlled access points (e.g., Guard, card access or CCTV with intercom). ✓ M ✓

#### 3.2. Limited access to dock areas

- 3.2.1. Only suppliers authorized employees and escorted visitors permitted access to dock/warehouse ✓ ✓ ✓

#### 3.3. High value storage area
### Supplier Facility/Truck Freight Security Requirements

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>= Requirement</td>
<td></td>
</tr>
<tr>
<td>✓ M</td>
<td>= Requirement &amp; mandatory to pass audit</td>
<td></td>
</tr>
<tr>
<td>✓ M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.3.1 Restricted-access, caged/vault area for assets on site more than 2 hours: High-grade security mesh, chain-link, or hard-wall, including top/roof; alarmed, CCTV, Card Access.

3.3.2 Restricted-access, caged/vault area for assets on site more than 6 hours: High-grade security mesh, chain-link, or hard-wall, including top/roof; CCTV, pad-locked.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.4 All external dock/warehouse doors secured

3.4.1 All external dock/warehouse doors secured unless required to be opened for normal transit operations.

3.5 CCTV coverage

3.5.1. Internal docks covered by CCTV

3.5.2. Buyer designated assets under 100% CCTV surveillance while in Supplier facility (this does not require 100% of floor coverage, rather 100% coverage of buyer's assets i.e., CCTV from dock, to pallet breakdown/buildup area, to HVP cage).

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ M</td>
<td>✓ M</td>
<td>✓ M</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ M</td>
<td>✓ M</td>
<td></td>
</tr>
</tbody>
</table>

3.6 Motion detection alarms

3.6.1 Motion detection alarms inside warehouse and activated when entire facility is vacated (N/A if facility is true 24x7x366 operation).

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ M</td>
<td>✓ M</td>
</tr>
</tbody>
</table>

### Security Systems

4.1 Monitoring of security systems

4.1.1 Manned security monitoring post 24x7x366; monitoring post secure from attack.

4.1.2 All security system alarms dealt with in real-time 24x7x366.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.2 Intruder alarm system

4.2.1 Minimum of 60 day records on system alarms.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Supplier Facility/Truck Freight Security Requirements</td>
<td>Applicable to Final Classification</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓M = Requirement &amp; mandatory to pass audit</td>
<td>✓</td>
</tr>
<tr>
<td>4.2.2 Restricted access to alarm system</td>
<td>✓</td>
</tr>
<tr>
<td>4.2.3 Monitoring of alarms by police or security contractor</td>
<td>✓</td>
</tr>
<tr>
<td>4.3 CCTV system</td>
<td>✓</td>
</tr>
<tr>
<td>4.3.1 All CCTV images are recorded in real time (VCR or digital-recording system). No more than 16 cameras to 1 tape/disk. If VCR, no more than 12 hours of images on one tape.</td>
<td>✓</td>
</tr>
<tr>
<td>4.3.2 Restricted access to CCTV system functions</td>
<td>✓</td>
</tr>
<tr>
<td>4.3.3 Minimum 30-day retention of all CCTV recordings; recordings are held in secure storage area</td>
<td>✓M</td>
</tr>
<tr>
<td>4.3.4 Preventative maintenance plan in place for CCTV systems (can be contracted or in-house).</td>
<td>✓</td>
</tr>
<tr>
<td>4.4 Card access system</td>
<td>✓</td>
</tr>
<tr>
<td>4.4.1 Minimum 60 days records on system transactions</td>
<td>✓</td>
</tr>
<tr>
<td>4.4.2 Restricted access to system functions</td>
<td>✓</td>
</tr>
<tr>
<td>4.4.3 Quarterly review of card access reports</td>
<td>✓</td>
</tr>
<tr>
<td>4.5 Security system maintenance</td>
<td>✓</td>
</tr>
<tr>
<td>4.5.1 Preventative maintenance plan in place to routinely test and service access control and alarm systems</td>
<td>✓</td>
</tr>
</tbody>
</table>

5. Security Procedures

5.1 Adequate documented security procedures

5.1.1 Local documented procedures for handling Buyer’s assets and escalation procedures for communicating security incidents to Buyer | ✓ | ✓ | ✓ |

5.1.2 Process for timely reporting of incidents of lost or missing Buyer’s assets. Incidents to be reported by the Supplier to the Buyer within 12 hours for missing assets | ✓ | ✓ | ✓ |
<table>
<thead>
<tr>
<th>Supplier Facility/Truck Freight Security Requirements</th>
<th>Applicable to Final Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓ M = Requirement &amp; mandatory to pass audit and 24 hours for lost assets.</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.3 Emergency customer and local management contacts for security incidents listed and available</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.4 Supplier Security Policy Statement available and communicated to all employees</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.5 Security awareness training (including robbery response training) for all dock, warehouse, Security and reception employees.</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.6 Employee and contractor ID picture badges required to be issued and worn</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.7 Procedures in place to restrict Supplier’s employees, visitors and contractors access to Buyer’s assets</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.8 Badge policy for visitors/contractors in place</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.9 Adequate control of paperwork. Restricting knowledge of transit of buyer’s assets to &quot;need to know&quot; only (Information Security).</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.10 At inbound checkpoint for drivers and crews, identity and authorization are validated</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.11 Keys controlled in areas where Buyers assets are transited / stored</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.12 Random trash inspection procedures in place for trash removal from dock/warehouse</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.13 Security incident reporting system and method of tracking local security incidents</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.14 Pre-loading or post-delivery storage of buyer’s assets in trailers</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.15 Personal containers (defined as lunch box, backpacks, coolers, purses, etc.) are controlled in the warehouse</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.16 Exit Searches performed on exit from secure areas used for Buyer assets</td>
<td>✓</td>
</tr>
<tr>
<td>Supplier Facility/Truck Freight Security Requirements</td>
<td>Applicable to Final Classification</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓M = Requirement &amp; mandatory to pass audit</td>
<td>✓</td>
</tr>
<tr>
<td>5.1.17 Personal vehicles access to shipping and receiving yard controlled.</td>
<td>✓</td>
</tr>
<tr>
<td>5.2. Background checks (vetting) within constraints of Local Country laws</td>
<td>✓M</td>
</tr>
<tr>
<td>5.2.1 Criminal history checks in place encompassing 5-year criminal history and employment check (vetting within constraints of local county laws).</td>
<td>✓</td>
</tr>
<tr>
<td>5.3. Terminated employees &amp; contractors procedure</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.1 Termination procedures in place for employees and contractors, ensuring return of ID's, access cards, keys and other sensitive information</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.2 Procedures in place preventing systems access to Buyer's data by terminated employees</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.3. Records kept preventing Supplier re-hiring terminated employee/contractor without considering previous background</td>
<td>✓</td>
</tr>
</tbody>
</table>


6.1 Adequate cargo truck security devices installed

<p>| 6.1.1 Solid-top, hard-sided, locked cargo doors or reinforced soft-sided trailer | ✓  | ✓  | ✓  |
| 6.1.2 Security tamper evident seals for trucks carrying Buyer only shipments | ✓  | ✓  | ✓  |
| 6.1.3 Vehicle immobilization devices in place | ✓  | ✓  |    |
| 6.1.4 Two way voice communications system between vehicle cab, Supplier's base (and escorts, if applicable) and procedures for reporting | ✓  | ✓  | ✓  |
| 6.1.5 Written contingency plans in place for reporting unscheduled events (i.e. stops, delays, route deviation) | ✓  | ✓  | ✓  |
| 6.1.6 Truck cabin and ignition keys secured from unauthorized use at all times. | ✓  | ✓  | ✓  |</p>
<table>
<thead>
<tr>
<th>Supplier Facility/Truck Freight Security Requirements</th>
<th>Applicable to Final Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓M = Requirement &amp; mandatory to pass audit</td>
<td></td>
</tr>
</tbody>
</table>

6.2. Scheduled routing

6.2.1 Routes, schedules and planned stops assessed for risk and reviewed ✓ ✓

6.3. Loading/unloading

6.3.1 Proof of shipping and receiving records (time, date, driver, shipping/receiving personnel, shipment details and quantity) ✓ ✓ ✓

6.3.2 When consignee allows, drive present at loading and unloading. ✓ ✓ ✓

7. Pre-Alerts

7.1 System of Pre-Alerts in place (Supplier to Supplier)

7.1.1 Pre-alert capability in place ✓ ✓

7.1.2 Destination to notify origin within 4 hours of receipt of shipment, reconciling pre-alert shipment details ✓

8. Enhanced Security Requirements

8.1 Driver training

8.1.1 Supplier to provide robbery response training, detailing safe and secure actions to be taken during the event driver is threatened. Details of training are to be available to Buyer ✓ ✓

8.1.2 Security Awareness training provided to drivers on mitigating risk. Details of training are to be available to buyer. ✓

8.2 Truck escorts (armed where local law permits) Cost shall be borne by Buyer

8.2.1 Capability to provide overt and covert escorts with real time communications to base and local police; written documentation in place ✓
<table>
<thead>
<tr>
<th>Supplier Facility/Truck Freight Security Requirements</th>
<th>Applicable to Final Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ = Requirement</td>
<td>A</td>
</tr>
<tr>
<td>✓M = Requirement &amp; mandatory to pass audit</td>
<td>✓</td>
</tr>
<tr>
<td>8.2.2 Documented response procedures and training for escort personnel</td>
<td></td>
</tr>
<tr>
<td>8.3 Vehicle tracking – subject to availability and negotiated between Buyer and Supplier</td>
<td>✓</td>
</tr>
<tr>
<td>8.3.1 GPS or similar technology installed on all vehicles transporting Buyer's assets.</td>
<td></td>
</tr>
</tbody>
</table>
Section 3 – Forms

Contents:
I. Request for Waiver

**FORM 3.1 – REQUEST FOR WAIVER**

| DATE OF REQUEST | SUPPLIER | Waiver #:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FACILITY LOCATION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAME OF PERSON REQUESTING WAIVER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POSITION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FREIGHT SECURITY REQUIREMENT FOR WHICH WAIVER IS BEING REQUESTED (ONE REQUIREMENT ONLY, USE ADDITIONAL REQUEST FORMS IF NECESSARY):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REASON FOR WAIVER REQUEST:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALTERNATIVE ACTIONS IMPLEMENTED OR PLANNED TO REDUCE RISK:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This Section For TAPA Use Only

Waiver Approved (Y/N)

Date Waiver Commenced

Date Waiver Expires (maximum 1 year)

Approved By (Name):

Approved By (Signature):

Date: Waiver Reference #