COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 27.2.2006
COM(2006)79 final

2006/0025(COD)

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on enhancing supply chain security

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on enhancing supply chain security

(SEC(2006)251)

(presented by the Commission)

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on enhancing supply chain security

1. The need for transport security

1.1 Terrorism is one of the greatest threats to democracy and freedom. The risk of a terrorist attack targeting freight transport remains high. The potential damage in terms of lives and economic activity is unfathomable and incalculable.

1.2. Transport security has become a vital worldwide issue. It concerns the European Union whose role as trading partner relies on effective and secure transport by all modes and at all levels. Its trading partners are beginning to address freight transport security issues. Indeed the United Stats has already introduced certain security measures for imports which have an impact on European supply chains.

1.3. Recently considerable improvements have been made to transport security in Europe: aviation and airport security have been given a European framework[1], maritime and port terminal security have been strengthened[2], and security within the entire port areas can be expected to improve considerably following the recent completion of the legislative process on security measures for seaports[3].

1.4. In 2003 the Commission already pointed to the need for enhanced security in land freight transport[4]. There are currently no rules in place for the European land transport supply chain in its entirety. The supply chain is defined as comprising all the transport and transport related operations and processes beginning at the production site and ending at the cargo's point of destination.

1.5. The threat of terrorist attacks has highlighted the vulnerabilities of the supply chain and the need to act: citizens expect to see security measures taken for the supply chain on which their daily lives depend and businesses can no longer afford to disregard security in order to protect their employees, their companies, their customers and the public from a terrorist attack.

1.6. To combat terrorism, the EU Heads of State called for "the strengthening of all forms of transport systems, including the enhancement of the legal framework and the improvement of preventive mechanisms."[5]

---

1 Regulation (EC) No °2320/2002, OJ L 355, 30.12.2002, p. 1.

2 Regulation (EC) No 725/2004, OJ L 129, 29.4.2004, p. 6.

3 Directive (EC) N°65/2005, JO L 310, 25.11.2005, p. 28.

4 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on enhancing maritime transport security, COM(2003) 229 final of 16.5.2003, p. 18.

5 Council of the European Union Declaration of 25 March 2004 on Combating Terrorism, document of Conseil 7906/2004 of 29 March 2004.

1.7. To do nothing is not an option. The Commission therefore proposes Community action to enhance the security in the land transport supply chain to complement existing Community transport security rules. This proposal does not cover passenger transport security, in particular in mass transport systems, which could be addressed at a later stage if necessary.

2. Towards improving supply chain security

2.1. In view of the need for urgent action and of the conclusions of the European Council, the Commission is submitting this Communication and a legislative proposal on enhancing supply chain security.

2.2. The Communication sets out the essential facts about freight transport security which any initiative in this area must take into account. It discusses the advantages and disadvantages of certain options and the reasons why the legislative measure proposed is the most realistic and focused approach to enhance security for European freight transport.

2.3 The goal of the proposal is to enhance supply chain security in order to provide greater protection for all European freight transport against possible terrorist attacks.

2.4. The objectives of the Commission's proposal are:

- to increase the level of security along the supply chain without impeding the free flow of trade;
- to establish a common framework for a systematic European approach without jeopardising the common transport market and existing security measures;
- to avoid unnecessary administrative procedures and burdens at European and national levels.

2.5. The measure proposed by the Commission:

- establishes a mandatory system requiring Member States to create a security ("secure operator") quality label which can be awarded to operators in the supply chain meeting European minimum security levels thus allowing mutual recognition of the label on the internal market;
- introduces, within the mandatory provisions for the Member States, a voluntary scheme under which operators in the supply chain increase their security performance in exchange for incentives ;
- makes operators in the supply chain responsible for their security performance in European freight transport;
- allows "secure operators" to benefit from facilitations where security controls are carried out and to distinguish themselves positively from other competitors in the area of security, giving them a commercial and competitive advantage;

- allows regular updating and upgrading of security requirements, including recognised international requirements and standards, through the committee procedure.

3. Key questions and the Commission's answers

What level of security is needed?

3.1 Two key links in many supply chains, namely air transport together with airports and maritime transport with seaports, have put in place intense levels of security in the form of rules and measures with detailed, legally binding specifications and checks. A similar approach for the remaining links in the supply chain would undoubtedly enhance security of the entire supply chain.

3.2. However, comparison of maritime and air transport with the supply chain as a whole reveals fundamental differences. The maritime and air transport markets are marked by a limited number of operators which, above all, operate in geographically confined and defined controllable areas. They are used to security arrangements.

3.3. The land transport supply chain as a whole has quite different dimensions. More than half a million[6] companies are involved in transport and ancillary services alone, ranging from major multinationals to tiny service companies rooted in a wide variety of cultures and business settings. They cover the entire Community. Most have no security management at present and, generally, security levels are only starting to develop.

3.4. The security awareness of all actors involved in the intra-EU supply chain should be increased. Depending on the goods transported, the position of the operator within the chain and the vulnerability of the infrastructure, the level of security needed can be defined. Highly prescriptive new security measures for all operators would lead to a breakdown of the supply chain. Yet an increasing number of companies are establishing their own security management standards not only to protect their own operations and brand but also as a tool for selecting their partners in the supply chain.

3.5. In view of the above, it is therefore impossible in practice to establish, in a single all-embracing operation, security rules and measures for the land transport supply chain comparable to those in air and maritime transport. Instead it is more realistic to establish a framework of minimum security requirements which can gradually evolve in line with technological progress and risk developments to ensure satisfactory security levels in an operational environment.

Security rules for containerised cargo only?

3.6. It is acknowledged that most current initiatives and deliberations are concentrating on containerised intermodal transport, both at national and international level and at the level of certain companies. This is understandable given the fears that a container

---

[6] Estimate according to EU Energy and Transport in Figures, Statistical Pocketbook 2004, chapter 3.1.12. This figure (for EU-25) does not include producers of goods which are at the start of a supply chain. Inclusion of them would take the total up to approx. 4,7 million companies in the supply chain.

might be misused for smuggling terrorist weapons or even as a delivery vehicle for a chemical, biological, radiological or nuclear weapon.

3.7. However, containers are not the only potential targets. Intra-European trade relies on various loading units which are all equally susceptible to terrorist interference. The same concern in fact applies to all types of cargo transport which, in one way or another, are at risk of misuse.

Security rules for specific areas or for the entire supply chain?

3.8. It is tempting to concentrate efforts on improving supply chain security levels in a limited number of clearly identified key areas: devices are being developed to make seals more resistant to tampering; most logistics centres have tightened access rules and many operators have introduced background checks and identity cards for employees. Risk awareness is growing.

3.9. All these developments are welcomed. But they are limited in scope and do not offer the systematic approach to supply chain security necessary to respond to potential terrorist risks or attacks as promptly and effectively as possible.

3.10. The supply chain is made up of a number of operations, beginning at the production site and ending at the cargo's point of delivery, and the processes accompanying them. These operations are interdependent, as are the operators which carry them out. All the individual elements, including the flows of information, have to pull together to ensure high levels of security along the entire supply chain.

3.11. However, improving security in well-defined key areas risks losing its impact if taken in isolation. The introduction of, e.g., secure seals would serve little useful purpose if not combined with appropriate developments in, e.g., security attitudes by personnel. Indeed, a fully secure part of the multi-operator supply chain where a specific security feature is of paramount importance would lose its security benefit if another part of the supply chain, with other security features, was allowed to remain insecure. At international level, only complete, secure supply chains receive recognition. The multitude of specific security features require tailor-made measures in response to the specificities of operators and supply chains.

3.12. In view of the foregoing, it is considered more appropriate to focus on the development of a Community security framework for the supply chain instead of opting for a patchwork approach. This choice by no means precludes detailed Community-wide minimum requirements or even detailed rules for certain areas. As will be explained later, the framework should contain such minimum requirements for all the individual links in the supply chain and specific technical rules where warranted. In all cases, however, the framework should allow regular, easy updates.

3.13. A framework would offer guidance to operators, which often make considerable investments into upgrading their security.

Who should be responsible for security ?

3.14. It has to be established whether one of the operators involved should be responsible for security of the entire supply chain or whether each operator should bear

responsibility for the security of its part of the supply chain. This point is relevant because the supply chain consists of a considerable number of operators.

3.15. The supply chain normally begins at the manufacturing site with the preparation for shipment. They may be loaded into containers or otherwise packed. They may be collected from the manufacturing site to be transported by a single mode to their final destination. They may be taken to warehouses, storage areas or inland terminals, where they may change transport modes. The operation may involve freight forwarders and agents or brokers. Every link in the supply chain is accompanied by often sophisticated information processes.

3.16. It is tempting to impose responsibility for the security of the complete supply chain on a single operator. This would be simple. But it would not reflect the reality of the market. It may well be that specialised manufacturers, due to their size and type of operation, carry out, or at least fully control, the transport operations. Their responsibility for the security of the entire supply chain may well be established.

3.17. However, in normal commercial circumstances, a manufacturer of goods does not carry out the complete transport operation. Specialised companies do that: railway companies are but one example. Indeed, manufacturers often do not know, nor do they even need to know, which operator transports their goods and by what means. The same considerations apply to other operators in the supply chain. They may control more than one link in the chain, or even, more rarely, the entire chain, except the first stage on the manufacturing site. Their responsibility may thus cover more than one stage.

3.18. These market realities point to only one practical conclusion: each operator of each link in the supply chain assumes responsibility for the security of its own – but only its own – activities. The individual security measures add up to the security of the complete chain.

3.19. Analysis of the supply chain identifies four groups of activities, each of which has its own security-relevant characteristics:

- preparation of goods for shipment and shipment from the production site;
- transport of goods;
- forwarding of goods;
- warehousing, storage and inland terminal operations.

How can existing EU concepts be used to increase security in the supply chain?

3.20. The Community customs rules[7] work with the concept of "authorised economic operator". Operators which comply with certain reliability criteria can be granted "authorised economic operator" status which allows them to benefit from facilitations with regard to safety and security-related customs controls and/or from simplifications provided for under customs rules. The latter is of particular

[7] Regulation (EC) N 648/2005, OJ L 117, 4.5.2005, p. 13.

commercial value to operators which can then control their material flow according to their own needs.

3.21. Under the Community's airport security regulation[8] a "regulated agent" or air carrier may recognise a consignor as a "known consignor" if the latter fulfils certain security-relevant criteria. As a result, certain security controls need not be applied to cargoes received from a "known consignor".

3.22. Both concepts are based on the underlying principle that operators which voluntarily comply with certain requirements and which have been vetted by the authorities should benefit from certain facilitations. They are regularly inspected. The same concept, with the appropriate changes, lends itself to supply chain security in the form of a "secure operator".

3.23. Specific minimum requirements should be set for operators involved in the four groups of activities:

- preparation of goods for shipment and shipment from the production site;
- transport of goods;
- forwarding of goods;
- warehousing, storage and inland terminal operations.

3.24. A "secure operator" scheme set up in the Member States would allow for operators in the supply chain to prove their compliance with minimum security requirements. The status of "secure operator" would be awarded to operators found to be in compliance with the requirements. For this purpose, Member States may avail themselves of existing systems or procedures or wish to create a system specifically earmarked for supply chain security. The implementation will need verifying; there cannot be trust without verification.

3.25. As it is impossible for the very substantial number of operators in the supply chain to implement the specific minimum requirements and for Member States to ensure that implementation is adequately verified, implementation will be on a voluntary basis. No operator will be forced to join the "secure operator" scheme.

3.26. In order to maintain the integrity of the common market, each Member State will have to recognise the "secure operator" status awarded by any other Member State, when the "secure operator" does business on its territory.

3.27. Where warranted, Member States may decide to limit access to installations and infrastructure to "secure operators".

---

[8] Regulation (EC) N° 2320/2002, OJ L 355, 30.12.2002, p. 1.

What advantages does the "secure operator" scheme offer?

3.28. Successful implementation of the "secure operator" scheme depends on tangible practical advantages for authorities and for those operators opting to make the financial investments:

3.28.1. Use of public resources. Authorities responsible for security would be able to concentrate their control resources on those operators which do not take part in the scheme without, however, forfeiting their right to control "secure operators", where warranted. The same approach proved successful when applied by customs authorities to their "authorised economic operators". There is no reason to believe that security authorities would not benefit from being able better to focus their work.

3.28.2. Europe-wide co-ordinated security drive. Authorities will be able, for the first time, to address Europe-wide supply chain security initiatives on the basis of common awareness, common objectives and common criteria.

3.28.3. Interconnectivity with secure maritime and air transport. Airports and seaports, including port facilities, which come under stringent Community security rules, can be confident that cargo entering their perimeter from a chain of "secure operators" has been adequately secured all along the chain. Such operators should be given preferential treatment, e.g. by being authorised to use "fast track treatment".

3.28.4. Europe-wide recognition. Europe-wide recognition of a "secure operator" status awarded by a national authority has advantages for the operators and the Member States: the operator will benefit from recognition throughout the EU. The Member States will be able to rely on awards by other Member States, knowing that the status has been granted on the basis of uniform European rules, applying agreed minimum European security requirements.

3.28.5. Integration into global supply chain security. With comparable security provisions, the customs authorities in charge of security controls at the external borders, both for exports and imports, will recognize for their "authorised economic operator" scheme, the status of a "secure operator" granted by the supply chain security authority. The supply chain security authority will do likewise with the "authorised economic operator". Current work by customs authorities and the conditions under the proposal annexed to this Communication, if implemented, will lead to compatibility and mutual recognition. The "secure operator" scheme would allow European exporters to benefit from current US import facilitation schemes, but also anticipates international developments. In fact, a European scheme could become a model for a rapid worldwide implementation of the global supply chain security recommendations developed by the World Customs Organisation.

3.28.6. Business security performance. The "secure operator" can demonstrate to its clients and its partners in the supply chain its ability to keep the supply chain free of security breaches. It will find it easier to identify responsible, security-conscious business partners to the detriment of others which are not security-conscious.

3.28.7. Business efficiency and resilience. Experience in adjacent areas points to the conclusion that operators can reap benefits from participating in the "secure operator" scheme. Implementation of the CSI scheme (US Container Security

Initiative) in maritime transport, although not specifically designed for operators to benefit from, is widely acknowledged to have had a number of positive commercial side-effects, notably better operational systems and better control over and predictability of transport and other processes, as well as more reliable processing times and reduced loss through theft. Trends in recently published research[9] indicate that a number of cost factors, both of the transport chain and of the businesses involved would draw positive collateral benefits in a number of areas from improved security measures.

Is a Community framework necessary?

3.29. Member States authorities wish to be assured that the same minimum security requirements apply in all Member States and that they are effectively implemented. After all, with the common market for supply chain operators a reality, every national authority will be confronted with operators having been granted "secure operator" status in another Member State expecting to be allowed to avail themselves of facilitations granted to national operators. National authorities must rely on uniform implementation of rules across Europe.

3.30. Although a high percentage of transport operations will always be restricted to the geographic confines of the European Union, a substantial portion also involve other European countries or countries outside Europe. Moves are already under way in non-EU countries with the aim of increasing supply chain security. Although the external dimension will necessarily involve custom authorities of both trade partners, national security systems will inevitably come under scrutiny. A uniform European system, implemented as soon as possible, is likely to have a considerable bearing on developments in non-EU countries and certainly more so than a disorganised patchwork of national rules.

3.31. The global aspects of supply chain security makes a Community framework necessary.

4. Conclusion

The Commission considers that a first step towards improving the security of the entire supply chain is needed. In view of the size and complexities of the market, a voluntary, but controlled framework for land transport supply chain security is the most appropriate course of action.

The framework will stimulate interconnectivity between the various modes of transport and operators, thereby enhancing security along the supply chain as a whole. "Fast track treatment" can stimulate national authorities to enhance co-operation between various administrative institutions and with industry, thus reducing administrative burdens.

---

[9] i.e. James B. Rice, Jr. and Philip W. Spayd, 'Investing in Supply Chain Security: Collateral Benefits', May 2005 (Massachusetts Institute of Technology) and Hau L. Lee and Seungjin Whang, 'Higher supply chain security with lower cost: Lessons from total quality management', International Journal of Production Economics, 2004.

The framework has to be put in place and can be further developed over time in line with the assessed security risks and the level of acceptance by commercial operators. It will encourage supply chain operators to introduce new security management tools and to improve existing ones in accordance with specific minimum requirements.

The voluntary element is underpinned by practical advantages in security controls, including those carried out by customs. It encourages innovative measures and allows participants to increase their competitiveness.

The proposal does not rule out stringent measures if it is shown that the market does not accept the proposed approach.

At legislative level, a proposal for a Regulation is enclosed.

EXPLANATORY MEMORANDUM

1. Context of the proposal

- **Grounds for and objectives of the proposal**

The EU Council identified transport as a key area in its fight against terrorism. It therefore called for "the strengthening of all forms of transport systems, including the enhancement of the legal framework and the improvement of preventive mechanisms[10]". This proposal is made in response to the needs identified and the Council's request.

- **General context**

Recently considerable improvements have been made to transport security in Europe: aviation and airport security have been given a European framework[11]; maritime transport[12] and port security[13] have been strengthened.

There are currently no rules in place for the Community land transport entire supply chain which is defined as comprising all the transport and transport-related operations and processes beginning at the production site and ending at the cargo's point of destination.

- **Existing provisions in the area of the proposal**

There are no existing provisions in the area of the proposal.

- **Consistency with other policies and objectives of the Union**

The proposal links up with existing transport security legislation. It is fully compatible with customs measures to increase transport security at the external borders and supports the objectives of the Lisbon agenda.

2. Consultation of interested parties and impact assessment

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

In December 2003 Member States, transport associations, trade unions, and other associations with a particular interest in transport and security, e.g. trade associations, were consulted on the basis of a consultation paper. Respondents represent a cross-section of industries both directly and indirectly concerned by transport security.

The open consultation was conducted over the internet from 23 December 2003 to 27 February 2004. The Commission received 65 responses. The results are available on http://europa.eu.int/comm/dgs/energy_transport/security/intermodal/consultation_en.htm

---

10 Council of the European Union Declaration of 25 March 2004 on Combating Terrorism, document of Conseil 7906/2004 of 29 March 2004.

11 Regulation (EC) N° 2320/2002, OJ L 355, 30.12.2002, p. 1

12 Regulation (EC) N°725/2004, OJ L 129, 29.4.2004, p. 6.

13 Directive (EC) N°65/2005, OJ L 310, 25.11.2005, p. 28.

The open consultation over the internet was followed by further consultations with Member States and industry during 2004 and the first half of 2005.

Summary of responses and how they have been taken into account

The key conclusions of the consultation process can be summarised as follows:

1) supply chain security has become a serious issue which needs addressing;

2) possible EU security measures should focus on terrorism rather than on crime in general;

3) risk assessment is important and should be further studied;

4) no guarantee of absolute security is likely to be achieved in the medium term;

5) the measures must take into account the realities of the market;

6) any measure should be EU wide so as to avoid distortion between markets and, as far as feasible, apply to all modes;

7) a single window approach for effective and similar control between various organisations and traders is appreciated, i.e. voluntary systems like the "regulated agent" and "known shipper" schemes.

These key conclusions are in line with the Commission approach to combat terrorism[14] form the bedrock of the Commission's proposal.

- **Collection and use of expertise**

The commission received expert advice from many sources: operators, business representatives, security and transport specialists and authorities in the Member States.

representatives, security and transport specialists and authorities in the Member States.

- **Impact assessment**

Alternative options have been investigated. A wide-ranging external study, 'The impact of possible European legislation to improve transport security', identified the fundamentals of the proposal as offering best value for money. The study is available at http://europa.eu.int/comm/dgs/energy_transport/security/intermodal/doc/2005_finalreport_impact_assessment_transport_security.pdf#pagemode=bookmarks

Member States

The proposal imposes an obligation on Member States to put in place a national system to award "secure operator" status to applicant operators which meet minimum requirements. Member States may either establish a new safety and security system or make use of existing ones. Although creation of a national scheme will require financial resources, it should be

[14] See notes 7, 9, 10, 11 and 12.

possible to harness synergies with existing security measures. The proposal allows the national authorities to operate the schemes on a cost-neutral basis.

Industries

The proposal contains no obligatory measures for supply chain operators. The "secure operator" scheme proposed is voluntary; its users can expect to benefit from security facilitations and simplifications of customs controls as well as portraying themselves as operators with high security standards to supply chain partners which require such standards. Other operators which believe that their activities do not require high security standards may decide not to take part in the new scheme.

Commission

None, except its obligation as guardian of the Treaties.

3. Legal elements of the proposal

- **Summary of the proposed action**

The Commission proposes that the European Parliament and the Council should adopt as soon as possible this Regulation on enhancing supply chain security. The proposal complements other transport security measures already in place.

The measures required for enhancing land transport supply chain security would follow these principles:

– supply chain security requires an active security partnership between Member State authorities and industry;

– supply chain security complements transport security measures already in place in the fields of aviation and maritime transport, including airports and seaports;

– an obligation for Member States to set up a national scheme to increase supply chain security which are compatible with each other;

– a voluntary framework for operators setting minimum requirements with which operators in four identified categories of supply chain operations must comply in order to be awarded the "secure operator" status;

– "Secure operators" should benefit from "fast track treatment" security facilitations and simplification of customs controls, and will enjoy enhanced standing with their commercial partners;

– Member States must designate a competent authority for supply chain security for granting "secure operator" status. They may appoint recognised organisations for supply chain security for this purpose provided these meet certain specified conditions;

– Member States must appoint a national focal point for supply chain security to handle the necessary communication both with other Member States and with the Commission;

– "Secure operator" status awarded by authorities in one Member State will be recognised by authorities in the other Member States;

– a procedure is laid down for adapting the provisions to technical change.

- **Legal basis**

Articles 71 and 80 (2) of the Treaty.

- **Subsidiarity principle**

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community. The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reasons:

- Common rules including a common framework are necessary to fight transnational terrorist risks effectively.

- Completion of the common transport market coupled with the Treaty's four freedoms requires a common European approach to supply chain security. A multitude of different national supply chain security schemes would risk recreating internal borders;

- Isolated initiatives taken by one or more Member States and necessarily resulting in diverging security levels between Member States would inevitably be interpreted by Europe's trading partners as unwillingness to address security issues or would be used to play off one Member State against another.

Community action will better achieve the objectives of the proposal. A Europe wide framework with identical minimum requirements for operators from all Member States will maintain a common security approach for the supply chain and avoid re-nationalising supply chain security.

This proposal is limited to what is necessary for a Community-wide framework:

– an identical approach, mandatory for the Member States to establish the common Community framework necessary to ensure the continued functioning of the transport market and voluntary for operators but clearly pointing to the necessity for all supply chain operators to improve security management;

– common minimum security requirements for the groups of operators working in the land transport supply chain; mutual recognition of "secure operator" status thus allowing all "secure operators" to benefit from facilitations and simplifications at national level and avoiding the risk of discrimination;

– a system that complements existing Community customs rules and allows updates to take account of international developments, e.g. in standardisation.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal is in line with the proportionality principle for the following reasons.

- The proposal is built on the realities of the supply chain. It avoids large scale highly prescriptive measures which would have been extremely difficult, if not impossible for Member States, to implement and control. Instead, it invites operators to invest in supply chain security knowing that their investment is in line with uniform Europe-wide requirements and offers the volunteers facilitations for security related controls and simplifications of possible procedural barriers;

- Member States, through the Council, have acknowledged the necessity to improve supply chain security;

- Member States can keep costs to the minimum. Member States would have to set up a scheme for awarding "secure operator" status for which they could, however, rely on already existing models in land transport safety and customs. They may seek practical assistance from recognised organisations for supply chain security. They may wish to decide to make the award procedure cost-neutral for the authorities. Regional and local authorities will not be involved, unless a Member State decides otherwise.

The costs are negligible for the Community: the Commission would only have to exercise its duties as guardian of the Treaty. Operators wishing to invest in security measures will now know that their investments are in line with Community-wide requirements. Trends in recently published research indicate that a number of cost factors, both of the transport chain and of the businesses involved would draw positive collateral benefits from improved security measures.

- **Choice of instruments**

Proposed instruments: Regulation. Other means would not be adequate for the following reasons.

Consideration was given to whether the Commission should propose a Regulation or a Directive. The choice of Regulation is fully in line with the security legislation: on maritime transport, aviation and airports. It is in line with the custom legislation which it could complement where the supply chain meets customs requirements.

The transnational risks of terrorism require a uniform, parallel and concurrent approach by Member States to establish a scheme which effectively counters the terrorist threat. A Regulation is the most effective tool.

Taken in isolation, the proposal is very simple; there is no need for general objectives and principles which could be fleshed out by Member States. The key elements can be implemented immediately to remedy the unsatisfactory security situation and, if based on a Regulation, without national implementing legislation.

A Regulation was therefore the most appropriate choice.

3. Budgetary implication

None.

4. Additional information

- **European Economic Area**

The proposed act is of EEA relevance and should therefore extend to the European Economic Area.

- **Detailed explanation of the proposal**

The Commission proposes to base the Regulation on Article 71 of the EC Treaty without prejudice to Member States' national security legislation and any measures that might be taken on the basis of Title VI of the Treaty on European Union.

SPECIAL CONSIDERATIONS:

Article 1:

This article sets out the objective of the Regulation.

Article 2:

This article defines 'supply chain'.

Article 3:

This article sets out the scope of the Regulation.

Article 4

This article imposes on Member States the obligation to designate a competent authority for supply chain security.

Article 5:

This article imposes on Member States the obligation to establish a national scheme to grant "secure operator" status to supply chain operators.

Article 6:

This article introduces the benefits of the "secure operator" status ("fast track treatment") and the possibility to refuse a "secure operator" the application of these benefits.

Article 7:

This article imposes the obligation of mutual recognition between Member States.

Article 8:

This article sets out the conditions under which "secure operator" status may be granted.

Article 9:

This article provides for the possibility to withdraw or suspend "secure operator" status.

Article 10:

This article places an obligation on Member States to set up award procedures, either directly through a public authority or through recognised organisations for supply chain security, and to make the list of "secure operators" accessible to national authorities, focal points and the Commission.

Article 11:

This article provides for appointing a focal point for supply chain security as the contact point for Member States and the Commission.

Article 12:

This article places an obligation on Member States to ensure adequate and regular supervision of their national schemes leading to granting "secure operator" status.

Article 13:

This article provides that the technical requirements contained in the Annexes to this Regulation may be amended or supplemented by the procedure laid down in Decision 1999/468/EC.

Article 14:

This article stipulates that the Commission will be assisted by a committee composed of representatives of the Member States.

Article 15:

This article concerns the confidentiality of security related information.

Article 16:

This article contains the details on entry into force.

Annex 1 - 4:

Contain the detailed requirements for a shipper, a transport company, a forwarding company, and a warehouse, storage facility or inland terminal to be awarded “secure operator” status.

Annex 5:

Contains the detailed requirements for operators to conduct a risk assessment.

Annex 6:

Contains the detailed conditions to be fulfilled by a recognised organisation for supply chain security.

2006/0025(COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on enhancing supply chain security

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 71 thereof,

Having regard to the proposal from the Commission[15],

Having regard to the opinion of the European Economic and Social Committee[16],

Having regard to the opinion of the Committee of the Regions[17],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[18],

Whereas:

(1) Security incidents and terrorism are among the greatest threats to the ideals of democracy and freedom and to the values of peace, which are the very essence of the European Union.

(2) The supply chain should be protected against security incidents. Such protection would benefit transport users, workers, the economy and the society as a whole.

(3) The European Council called for "the strengthening of all forms of transport systems, including the enhancement of the legal framework and the improvement of preventive mechanisms"[19].

(4) Recently considerable improvements have been made to transport security in Europe for aviation[20] and maritime transport.[21] Further improvements are expected following the recent adoption of security measures for ports[22].

---

15 OJ C […], […], p. […].
16 OJ C […], […], p. […].
17 OJ C […], […], p. […].
18 OJ C […], […], p. […].
19 Council of the European Union Declaration on Combating Terrorism of 25 March 2004, document of Conseil 7906/2004 of 29 March 2004.
20 Regulation (EC) N°2320/2002, OJ L 355, 30.12.2002, p. 1.
21 Regulation (EC) N°725/2004, OJ L 129, 29.4.2004, p. 6.
22 Directive (EC) N°65/2005, OJ L 310, 25.11.2005, p. 28.

(5) Supply chain security levels outside the above-mentioned areas remain unsatisfactory without Community rules in place.

(6) It is necessary to improve the security level of the European land transport supply chain. This should be achieved by adopting appropriate measures without prejudice to the rules of the Member States in the fields of national security and measures which might be taken on the basis of Title VI of the Treaty on European Union.

(7) Any measure must take account of the supply chain markets which are made up by a vast number of operators and operating models which render measures comparable to those in aviation and maritime transport inappropriate in the short term.

(8) Any measure should ensure a free flow of trade whilst allowing tightening of minimum security requirements.

(9) Member States should introduce a scheme under which they award "secure operator" status to Community-based operators in the supply chain provided the operators meet certain minimum security requirements. This scheme should be compatible with supply chain security programmes being developed for global supply chains.

(10) Supply chain operators fall into one of the following groups: preparation and shipment of goods from the production site; transport of goods; forwarding of goods; warehousing, storage and inland terminal operations.

(11) Minimum security requirements should be specified for each of the groups of supply chain operators. Member States may introduce higher requirements for operators established on their territory.

(12) A "secure operator" scheme would provide advantages for authorities and commercial operators.

(13) A "secure operator" scheme would allow authorities responsible for security to concentrate their control resources on those operators not ready to meet minimum security requirements and to do so in the context of a common Europe-wide security drive.

(14) The "secure operator" status shall be recognised throughout the European Union.

(15) Member States should grant "secure operators" facilitations in the area of security controls plus simplifications of security controls at external borders, including where available, the use of "fast track treatment", without losing the right to carry out security controls on "secure operators".

(16) "Secure operators" would furthermore be able to demonstrate to the market their ability to keep the supply chain free of security breaches, to distinguish themselves positively from other operators and to establish a positive trend in business security performance.

(17) Member States should ensure that a list of "secure operators" is made accessible to other Member States' authorities and the Commission.

(18) "Secure operator" status should be recognized throughout the European Union but could be withdrawn by the Member State which awarded it if the operator were found to be in serious breach of the conditions under which it was awarded. The status should be for a limited time but renewable. A Member State may refuse to grant facilitations and simplification where it finds that a "secure operator" which has been awarded this status by another Member State is in breach of the minimum security requirements.

(19) Member States could appoint recognised organisations for supply chain security for the purpose of assessing whether an applicant "secure operator" meets the required conditions.

(20) Member States should appoint a competent authority for supply chain security.

(21) Member States should ensure that a focal point assumes the role of contact point between the Commission and the Member States.

(22) Member States should monitor implementation among supply chain operators.

(23) The measures needed to implement this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[23]. A procedure should be defined for adaptation of this Regulation to take account of developments in international instruments and, in the light of experience, to adapt or supplement the detailed provisions of the annexes to this Regulation, without changing the scope of this Regulation.

(24) The objectives of the proposed action, namely the introduction of a common approach to supply chain security, a common "secure operator" scheme and the necessity to ensure recognition of nationally awarded "secure operator" status throughout the entire common transport market can, by reason of the European scale of this Regulation, be better achieved at Community level. Therefore, the Community may adopt measures in accordance with the principle of subsidiarity set out in Article 5 of the Treaty. In accordance with the principle of proportionality set out in the same Article, this Regulation is limited to the minimum security requirements required to achieve the objectives of supply chain security and does not go beyond what is necessary for that purpose.

HAVE ADOPTED THIS REGULATION:

Article 1

Objective

1. This Regulation establishes common rules for enhancing land transport supply chain security in the face of threats of security incidents.

2. The objective set in paragraph 1 shall be achieved by means of:

[23] OJ L 184, 17.7.1999, p. 23.

a) setting up a scheme which enables Member States to award the "secure operator" status to operators in the supply chain;

b) setting minimum security requirements which operators have to meet before they can be awarded the "secure operator" status;

c) setting up appropriate monitoring mechanisms.

Article 2

Definition

For the purpose of this Regulation supply chain means all the processes and operators involved in the preparation for transport and the land transport of goods from the production site to the point of delivery within the territory of the European Community.

Article 3

Scope

1. This Regulation shall apply to supply chain security and addresses the security of cargo, transport and, where appropriate, infrastructure related to the supply chain within the territory of the European Community.

2. The measures laid down in this Regulation shall apply to any operator involved in one of the following activities:

   a) preparation of goods for shipment and shipment of goods from the production site;

   b) transport of goods;

   c) forwarding of goods;

   d) warehousing, storage or inland terminal operations.

3. The Regulation shall apply without prejudice to:

   a) Community rules in the field of civil aviation security[24];

   b) Community rules on enhancing ship and port facility security[25];

   c) Community rules on port security [26];

   d) Community and international rules on the transport of dangerous goods[27] and nuclear material[28];

---

24 Regulation (EC) N° 2320/2002, OJ L 355, 30.12.2002, p. 1.
25 Regulation (EC) N° 725/2004, OJ L 129, 29.4.2004, p. 6.
26 Directive (EC)N°65/2005, OJ L 310, 5.11.2005, p. 28.

e) Community customs rules[29].

Article 4

Competent authority for supply chain security

Member States shall designate a competent authority for supply chain security to coordinate, implement and monitor application of the supply chain security measures laid down in this Regulation.

Article 5

"Secure operator"

1. Within 18 months of the adoption of this Regulation, Member States shall establish a scheme to award "secure operator" status to operators in the supply chain.

2. An operator may apply to be awarded "secure operator" status provided it is involved in one of the following activities in the supply chain:

   a) preparation of goods for shipment and shipment of goods from the production site;

   b) transport of goods;

   c) forwarding of goods;

   d) warehousing, storage or inland terminal operations.

3. The application shall be addressed to the competent authority for supply chain security in the country where the applicant is established.

4. "Secure operator" status demonstrates the ability of the operator to which it is awarded to keep the part of the supply chain under its responsibility free of security breaches.

5. Member States shall inform the European Commission once their scheme to award "secure operator" status is in place.

---

27 Council Directive 94/55/EC of 21 November 1994, as amended, on the approximation of the laws of the Member States with regard to the transport of dangerous goods by road - OJ L 319, 12.12.1994, p. 7. Council Directive 96/49/EC of 23 July 1996 on the approximation of the laws of the Member States with regard to the transport of dangerous goods by rail – OJ L 235, 17.9.1996, p. 25. Council Directive 1999/36/EC of 29 April 1999 on transportable pressure equipment - OJ L 138, 1.6.1999, p. 20.

28 EC Council Directive 2003/122/Euratom of 22 December 2003 on the control of high-activity sealed radioactive sources and orphan sources, OJ L 346, 31.12.2003, p. 57.

29 Regulation (EC) No. 648/2005, OJ L 117, 4.5.2005, p. 13.

Article 6

"Secure operator's" benefits

1. Member States shall allow "secure operators" to benefit from facilitations and simplifications related to security control measures ("fast track treatment").

2. Facilitation and simplifications shall include permission for "secure operators" to move their cargoes following procedures which set them aside from operators which are not secure. These shall include a reduced level of security controls.

3. Member States may verify the authenticity of "secure operator" status with the competent focal point.

4. A Member State may refuse application of article 6(1) and 6(2) to a "secure operator" of another Member State when this operator is found to be in serious breach of security rules. It shall inform the other Member States and the Commission forthwith and shall bring the matter before the committee set up by Article 14. Articles 9 and 12 shall apply.

Article 7

Mutual recognition

"Secure operator" status awarded in one Member State shall be recognised by the authorities in all Member States.

Article 8

Award of status

1. An operator shall be awarded "secure operator" status if it shows that

   a) it has established, implemented, and documented a security management system;

   b) it ensures that resources to counter possible security risks are made possible to that part of the supply chain for which it bears responsibility;

   c) its security management system allows continuous improvements;

   d) it meets the specific requirements provided for in the annexes.

   e) it meets the requirements under the rules referred to in article 3(3), where applicable.

2. "Secure operator" status shall be awarded for periods of three years. The status may be renewed where the "secure operator" continues to meet the minimum requirements of this Regulation.

3. If an operator has been granted the status of "authorised economic operator" in accordance to article 5a of EC Regulation No. 648/2005[30], the competent authority for supply chain security shall consider the criteria described in paragraph 1 met, under the condition that the criteria for granting the "authorised economic operator" status are identical or comparable.

Article 9

Withdrawal or suspension of status

1. Member States shall introduce rules which allow withdrawal of "secure operator" status where the operator is found to be in serious or repeated breach of the conditions under which the status was awarded.

2. "Secure operator" status may also be withdrawn as a result of implementation and conformity checks carried out in accordance with Article 12.

3. Where the "secure operator" status is withdrawn, the operator may re-apply only after two years.

4. Member States shall introduce rules which allow for the suspension of "secure operator" status where the operator is found to be in other breaches of the conditions under which the status was awarded.

5. The suspension shall be lifted when the competent authority for supply chain security is satisfied that the breaches have been remedied.

Article 10

Award procedures

1. The competent authority for supply chain security shall be responsible for awarding "secure operator" status. Member States shall establish a register of all "secure operators". The register shall be accessible to the Member States' competent authorities for supply chain security and focal points and to the Commission.

2. Each "secure operator" shall be given an identification number beginning with the Member State's country code.

3. Member States may appoint recognised organisations for supply chain security for the purpose referred to in paragraph 1. The recognised organisations for supply chain security shall meet the conditions set out in Annex 6.

[30] OJ L 117, 4.5.2005, p. 13.

Article 11

Focal point for supply chain security

1. Member States shall appoint a focal point for supply chain security.

2. The focal point shall serve as the contact point for the Commission and other Member States and shall facilitate, follow and inform on the application of supply chain security measures.

Article 12

Implementation and conformity checking

Member States shall ensure adequate monitoring of the "secure operator" scheme including the supervision of the recognised organisations for supply chain security.

Article 13

Adaptation

The provisions of the annexes may be amended or supplemented by detailed technical requirements in accordance with the procedure referred to in Article 14, without changing the scope of this Regulation.

Article 14

Committee procedure

1. The Commission shall be assisted by a committee composed of representatives of the Member States and chaired by a representative of the Commission.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC[31] shall apply, having regard to the provisions of Article 8 thereof.

3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at one month.

4. The committee shall adopt its rules of procedure.

[31] OJ L 184, 17.7.1999, p. 23.

Article 15

Confidentially and dissemination of information

1. In applying this Regulation, the Commission shall take appropriate measures, in accordance with Commission Decision 2001/844/EC, ECSC, Euratom[32], to protect information subject to the requirements of confidentiality to which it has access or which is communicated to it by Member States.

2. The Member States shall take equivalent measures in accordance with relevant national legislation.

Article 16

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

[32] OJ L 317, 3.12.2001, p. 1.

ANNEX 1

Shipper

(preparation of goods for shipment and shipment from the production site)

For a shipper to be awarded "secure operator" status, its security management system must be based on a risk assessment and address the following:

Physical security: All buildings and premises should be protected against unauthorised entry and protect against outside intrusion. Physical security should include:

- Locking devices for external and internal doors, windows, gates, and fences;
- Lighting inside and outside the facility, including parking areas;
- Parking area for private vehicles separate from the shipping, loading, and cargo areas;
- Internal/external communications systems to contact internal security personnel or local law enforcement agencies.

Access controls: Unauthorised access to the shipping, loading and cargo areas should be prohibited. Controls should include:

- Systematic fail-proof identification of all employees, visitors and business contacts;
- Procedures for challenging unauthorised/unidentified persons.

Procedural security: Measures for handling incoming and outgoing goods should include protection against the introduction, exchange or loss of material. Security procedures should include:

- A designated security officer to supervise the introduction/removal of cargo;
- Properly marked, weighed, counted, and documented cargo;
- Controlling the integrity of seals or other security devices of incoming cargo;
- Procedures for putting seals or other security devices on outgoing cargo;
- Detecting and reporting shortages and surpluses;
- Tracking the movement of incoming and outgoing goods;
- Proper storage of empty and full loading units to prevent unauthorised access;

- Procedures to address anomalies or illegal activities which are detected or suspected by the company.

Personnel security: Companies should establish an internal process to screen prospective employees, and verify applications, in full respect of the legislation in the areas of equal treatment and personal data protection. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Documentation procedures: Companies should ensure that documentation is complete, legible, accurate and submitted in time.

Information security: All information processes in the context of supply chain operations must be secured.

Education and training awareness: A security awareness programme should be provided to employees including recognizing possible security risks, maintaining product integrity, and determining and addressing unauthorised access. These programmes should encourage active employee participation in security controls.

ANNEX 2

Transport company

For a transport company to be awarded "secure operator" status, its security management system must be based on a risk assessment and address the following:

Physical security: All buildings, premises and means of transport should be protected against unauthorised entry and protect against outside intrusion. Physical security should include:

- Locking devices on external and internal doors, windows, gates and fences;
- Perimeter fencing, adequate lighting inside and outside the facility, including the parking areas;
- Parking area for private vehicles separate from the shipping, loading, and cargo areas;
- Internal/external communications systems to contact internal security personnel or local law enforcement agencies;

Access controls: Unauthorised access to facilities and means of transport should be prohibited. Controls should include:

- Systematic fail-proof identification of all employees, visitors, and business contacts;
- Procedures for challenging unauthorised/unidentified persons;

Procedural security: Procedures should be in place to protect against undocumented material being introduced aboard the means of transport and into cargoes and to protect against unauthorised personnel being allowed access. Security procedures should include:

- Properly marking, counting, and documenting of cargo/cargo equipment;
- Controlling the integrity of seals and other security devices when cargo is accepted for transport;
- Procedures for assuring the integrity of seals and other security devices when cargo is handed over;
- A system for detecting and reporting shortages;
- Tracking the movement of incoming and outgoing goods and means of transport;
- Procedures to address anomalies or illegal activities which are detected or suspected by the company.

In cases where undocumented materials or signs of tampering are discovered, a physical inspection of accessible parts of the means of transport and of readily accessible areas near the means of transport should be carried out. Procedures for reporting these cases should be in place.

Personnel security: Companies should establish an internal process to screen prospective employees, and verify applications, in full respect of the legislation in the areas of equal treatment and personal data protection. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Documentation procedures: Companies should ensure that documentation is complete, legible, accurate and submitted in time.

Information security: All information processes in the context of supply chain operations must be secured.

Secure freight flow provisions: Companies may upgrade cargo being offered by non "secure operators" as secure when inspection of the content allows them to do so. If such inspections do not take place or do not allow cargo to be considered part of a secure supply chain "fast track treatment" may be refused.

Education and training awareness: A security awareness programme should be provided to employees including recognising possible security risks, maintaining product integrity, and determining and addressing unauthorised access. These programmes should encourage active employee participation in security controls.

ANNEX 3

Forwarding company

For a forwarding company to be awarded "secure operator" status, its security management system must be based on a risk assessment and address the following:

Access Controls: Unauthorised access to the facilities should be prohibited. Controls should include the positive identification of all employees, visitors, and business contacts as well as procedures for challenging unauthorised and unidentified persons.

Procedural Security: Procedures should address anomalies or illegal activities which are detected or suspected by the company.

Documentation Processing: Forwarding companies should make their best efforts to ensure that all documentation provided and used in the clearing of cargo is legible and protected against the exchange, loss or introduction of erroneous information. Documentation procedures should include:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity and unit of measure (i.e. boxes, cartons, etc.) of the cargo;
- Recording, reporting, and investigating shortages and surpluses of cargo;
- Tracking the movement of incoming and outgoing cargo;
- Safeguarding computer access and information.

Personnel security: Companies should establish an internal process to screen prospective employees, and verify applications, in full respect of the legislation in the areas of equal treatment and personal data protection. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Documentation procedures: Companies should ensure that loading lists, manifests and/or other transport related documents are complete, legible, accurate and submitted in time.

Information Security: All information processes in the context of supply chain operations must be secured.

Secure freight flow provisions: Companies may upgrade cargo being offered by non – "secure operators" as secure when inspection of the content allows them to do so. If such inspections do not take place or do not allow cargo to be considered part of a secure supply chain "fast track treatment" may be refused.

Education and training awareness: A security awareness programme should be provided to employees including recognizing possible security risks, maintaining cargo integrity, and determining and addressing unauthorised access. These programmes should encourage active employee participation in security controls and should provide:

- Recognition for active employee participation in security controls;
- Training in documentation fraud and computer security controls.

ANNEX 4

Warehouse, storage facility or inland terminal operations (including inland ports*)

For a company operating a warehouse, storage facility, inland terminal or an inland port to be awarded "secure operator" status, its security management system must be based on a risk assessment and address the following:

Physical Security: All buildings should be constructed of materials, which resist unauthorised entry and protect against outside intrusion. Physical security should include:

- Locking devices for external and internal doors, windows, gates and fences;
- Lighting provided inside and outside the facility, including parking areas;
- Parking area for private vehicles separate from the shipping, loading, and cargo areas;
- Internal/external communications systems in place to contact internal security personnel or local law enforcement police.

Access controls: Unauthorised access to facilities should be prohibited. Controls should include:

- Systematic fail-proof identification of all employees, visitors, and business contacts;
- Procedures for challenging unauthorised/unidentified persons.

Procedural security: Procedures should be in place to protect against undocumented material being introduced into the warehouse, storage facility or inland terminal (incl. inland ports). Security procedures should include:

- A designated security officer to supervise the introduction/removal of cargo;
- Properly marked, counted, and documented cargo and equipment verified against manifest documentation;
- Controlling the integrity of seals and other security devices on incoming cargo;
- Procedures for putting seals and other security devices on outgoing cargo;
- Procedures for detecting and reporting shortages and surpluses;
- Procedures to address anomalies or illegal activities which are detected or suspected by the company;
- Proper storage of empty and full loading units to prevent unauthorised access;

- Prevention of access to cargo or empties.

Personnel security: Companies should establish an internal process to screen prospective employees, and verify applications, in full respect of the legislation in the areas of equal treatment and personal data protection. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Information security: All information processes in the context of supply chain operations must be secured.

Secure freight flow provisions: Companies may upgrade cargo being offered by non – "secure operators" as secure when inspection of the content allows them to do so. If such inspections do not take place or do not allow cargo to be considered part of a secure supply chain "fast track treatment" may be refused.

Education and training awareness: A security awareness programme should be provided to employees including recognizing possible security risks, maintaining cargo integrity, and determining and addressing unauthorised access. These programmes should encourage active employee participation in security controls.

* Provided Regulation (EC) 725/2004 does not apply.

ANNEX 5

Risk assessment

The risk assessment of an operator should lead to a security management system. The risk assessment must be based on the general situation of the company, not on a specific transport operation, and address at least the following steps:

Step one - Identifying the types of threat:

- The actual news coverage of the current national and international climate, or current terrorist campaigns;
- The security authorities' advice on the risk of a terrorist attack on facilities or operations;
- The attractiveness of the organisation's building, operations or staff for a terrorist attack;
- The possibility of collateral damage in view of the operator's location in a high-risk neighbourhood.

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

Step three - Identifying what should be done to reduce the risk to an acceptable level.

ANNEX 6

Conditions to be met by a recognised organisation for supply chain security

A recognised organisation for supply chain security should be able to demonstrate:

- An unblemished corruption and anti-fraud record, both for the organisation and its employees;
- Expertise in relevant aspects of supply chain security;
- An appropriate knowledge of supply chain operations, including knowledge of operational requirements;
- An appropriate knowledge of other security relevant operations potentially affecting supply chain security;
- The capability to assess the likely supply chain security risks;
- The ability to maintain and improve the supply chain security expertise of its personnel;
- The ability to monitor the continuing trustworthiness of its personnel;
- The ability to maintain appropriate measures to avoid unauthorised disclosure of, or access to, security-sensitive material;
- Knowledge of relevant national and international legislation and security requirements;
- Knowledge of current security threats and patterns;
- Knowledge of recognition and detection of weapons, dangerous substances and devices;
- Knowledge of recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten supply chain security;
- Knowledge of techniques used to circumvent security measures;
- Knowledge of security and surveillance equipment and systems and their operational limitations.

LEGISLATIVE FINANCIAL STATEMENT

1. NAME OF THE PROPOSAL :

Regulation of the European Parliament and of the Council on enhancing supply chain security.

2. ABM / ABB FRAMEWORK

Policy area(s) concerned and associated Activity/Activities:

Policy area(s): Inland, air and maritime transport policy

Activit(y/ies): Implementation and monitoring of supply chain security measures.

3. BUDGET LINES

3.1. Budget lines (operational lines and related technical and administrative assistance lines (ex- B.A lines) including headings :

06 02 03 02 Transport security

06 02 11 03 Committees

3.2. Duration of the action and of the financial impact:

Indefinite, starting in 2008

3.3. Budgetary characteristics (add rows if necessary) :

Budget line	**Type of expenditure**		**New**	**EFTA contribution**	**Contributions from applicant countries**	**Heading in financial perspective**
	Non-comp	NDA	NO	NO	NO	**No**
	Non-comp	NDA	NO	NO	NO	**No**

4. SUMMARY OF RESOURCES

4.1. Financial resources

4.1.1. Summary of commitment appropriations (CA) and payment appropriations (PA)

EUR million (to 3 decimal places)

Expenditure type	Section No.		2006	2007	2008	2009	2010	2011 and later	Total
Operational expenditure[33]									
Commitment appropriations (CA)	8.1	a	0	0	0	0.	0.5	0	0.5
Payment appropriations (PA)		b	0	0	0	0.	0.5	0	0.5
Administrative expenditure within reference amount[34]									
Technical & administrative assistance (NDA)	8.2.4	c	0	0	0	0	0	0	0
TOTAL REFERENCE AMOUNT									
Commitment appropriations		**a+c**	0	0	0	0.	0.5	0	0.5
Payment appropriations		**b+c**	0	0	0	0.	0.5	0	0.5
Administrative expenditure <u>not</u> included in reference amount[35]									
Human resources and associated expenditure (NDA)	8.2.5	d	0	0	0	0	0	0	0
Administrative costs, other than human resources and associated costs, not included in reference amount (NDA)	8.2.6	e	0	0	0.056	0.037	0.037	0.037	0.168
Total indicative financial cost of intervention									
TOTAL CA including cost of human resources		a+c +d+ e	0	0	0.056	0.037	0.537	0.037	0.668
TOTAL PA including cost of human resources		b+c +d+ e	0	0	0.056	0.037	0.537	0.037	0.668

33 Expenditure that does not fall under Chapter xx 01 of the Title xx concerned.

34 Expenditure within article xx 01 04 of Title xx.

35 Expenditure within chapter xx 01 other than articles xx 01 04 or xx 01 05.

Co-financing details

If the proposal involves co-financing by Member States, or other bodies (please specify which), an estimate of the level of this co-financing should be indicated in the table below (additional lines may be added if different bodies are foreseen for the provision of the co-financing):

EUR million (to 3 decimal places)

Co-financing body		2006	2007	2008	2009	2010	2011 and later	Total
……	f							
TOTAL CA including co-financing	a+c +d+ e+f	0	0	0	0	0	0	0

4.1.2. Compatibility with Financial Programming

X Proposal is compatible with existing financial programming.

☐ Proposal will entail reprogramming of the relevant heading in the financial perspective.

☐ Proposal may require application of the provisions of the Interinstitutional Agreement[36] (i.e. flexibility instrument or revision of the financial perspective).

4.1.3. Financial impact on revenue

X Proposal has no financial implications on revenue

☐ Proposal has financial impact – the effect on revenue is as follows:

NB: All details and observations relating to the method of calculating the effect on revenue should be shown in a separate annex.

[36] See points 19 and 24 of the Interinstitutional agreement.

EUR million (to one decimal place)

		Prior to action	Situation following action					
Budget line	Revenue	[Year n-1]	[Year n]	[n+1]	[n+2]	[n+3]	[n+4]	[n+5][37]
	a) Revenue in absolute terms							
	b) Change in revenue	*Δ*						

(Please specify each revenue budget line involved, adding the appropriate number of rows to the table if there is an effect on more than one budget line.)

4.2. Human Resources FTE (including officials, temporary and external staff) – see detail under point 8.2.1.

Annual requirements	2007	2008	2009	2010	2011	2012
Total number of human resources	0	0	0	0	0	0

5. CHARACTERISTICS AND OBJECTIVES

Details of the context of the proposal are required in the Explanatory Memorandum. This section of the Legislative Financial Statement should include the following specific complementary information:

5.1. Need to be met in the short or long term

In its Anti-Terrorism Declaration of 25 March 2004[38], the European Council "calls for the strengthening of all forms of transport systems, including the enhancement of the legal framework and the improvement of preventive mechanism." This proposal is in response to the needs identified and the Council's request.

In recent years, the European Union has made considerable progress towards protecting its transport operations from the terrorist threat. European security legislation is in place for aviation, including airports, and maritime transport. Legislation on securing seaports has reached the end of the legislative process. There is no European legislation covering

[37] Additional columns should be added if necessary i.e. if the duration of the action exceeds 6 years.

[38] Council of the European Union Declaration of 25 March 2004 on Combating Terrorism, document of Conseil 7906/2004 of 29 March 2004.

the supply chain outside the areas referred to above. This proposal bridges the existing security gaps between the various transport modes.

5.2. Value-added of Community involvement and coherence of the proposal with other financial instruments and possible synergy

In order to avoid the re-emergence of national transport markets, due to national supply chain security rules, a Community approach is required, as has been the case for maritime transport, seaports, aviation and airports.

5.3. Objectives, expected results and related indicators of the proposal in the context of the ABM framework

None, except existing function as guardian of the Treaties.

5.4. Method of Implementation (indicative)

Show below the method(s)[39] chosen for the implementation of the action.

- ☐ ***Centralised Management***
  - ☐ Directly by the Commission
  - ☐ Indirectly by delegation to:
    - ☐ Executive Agencies
    - ☐ Bodies set up by the Communities as referred to in art. 185 of the Financial Regulation
    - ☐ National public-sector bodies/bodies with public-service mission
- ☐ ***Shared or decentralised management***
  - ☐ With Member states
  - ☐ With Third countries
- ☐ ***Joint management with international organisations (please specify)***

Relevant comments:

None.

[39] If more than one method is indicated please provide additional details in the "Relevant comments" section of this point.

6. MONITORING AND EVALUATION

6.1. Monitoring system

The Commission will have to carry out conventional monitoring work as guardian of the Treaties.

6.2. Evaluation

6.2.1. Ex-ante evaluation

The European Council's Anti-Terrorism Declaration of 25 March 2004[40] set the imperative political context of this Commission initiative.

From 2004 a consultation process took place. This process sharpened the focus of possible EU measures to enhance land transport supply chain security was developed and was verified with Member States and stakeholders.

The consultation process and the impact assessment[41] indicate that EU measures should take account of the following:

- Supply chain security is about thinking the unthinkable. Security risks relate to cargo, transport modes and infrastructure. Total security can never be guaranteed by public authorities.

- Many companies are increasingly implementing their own security standards. Their supply chain partners have to adjust to these procedures. Transport service providers and other suppliers who work for a number of clients face being subjected to multiple assessments, which is unnecessary, disruptive and costly.

- The challenge is to achieve the highest possible level of security for the supply chain without jeopardizing trade whilst keeping administrative requirements to the minimum.

- Public authorities and industry need to co-operate to enhance supply chain security. The guiding principle is that operators which voluntarily comply with certain requirements and which have been vetted by the authorities should benefit from certain facilitations and simplifications.

---

40 Council of the European Union Declaration on Combating Terrorism, document of Conseil 7906/2004 of 29 March 2004.

41 DNV Consulting, 'Study on the impacts of possible legislation to improve transport security'. Costs under 2004 budget.

- A uniform supply chain framework approach will reduce security related competition within EU boundaries. Certification of companies might be an option.

6.2.2. Measures taken following an intermediate/ex-post evaluation (lessons learned from similar experiences in the past)

The Commission intends to order a study to evaluate the impact and the effectiveness of the measures adopted. Such a study should be conducted in 2010, and then every three years. Such regular evaluation is necessary to enable the Commission to propose, via the committee procedure, any adjustments to the proposed system which might prove necessary. The unit cost of each study is estimated at €500.000.

6.2.3. Terms and frequency of future evaluation

See 6.2.2.

7. ANTI-FRAUD MEASURES

Under annex 6 to the proposed Regulation a recognised security organisation for supply chain security must demonstrate an unblemished corruption and anti-fraud record, both for the organisation and its employees.

8. DETAILS OF RESOURCES

8.1. Objectives of the proposal in terms of their financial cost

Commitment appropriations in EUR million (to 3 decimal places)

(Headings of Objectives, actions and outputs should be provided)	**Type of output**	**Av. cost**	**2006**		**2007**		**2008**		**2009**		**2010**		**2011**		**TOTAL**	
			No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost
OPERATIONAL OBJECTIVE No.1 [42]																
Action 1																
Output 1																
Output 2																
Action 2.																
Output 1																
Sub-total Objective 1																
OPERATIONAL OBJECTIVE No.2 [1]																
Action 1																
Output 1																
Sub-total Objective 2																
OPERATIONAL OBJECTIVE No.n [1]																
Sub-total Objective n																
TOTAL COST																

[42] As described under Section 5.3.

8.2. Administrative Expenditure

8.2.1. Number and type of human resources

Types of post		Staff to be assigned to management of the action using existing and/or additional resources (**number of posts/FTEs**)					
		2006	2007	2008	2009	2010	2011
Officials or temporary staff[43] (XX 01 01)	A*/AD						
	B*, C*/AST						
Staff financed[44] by art. XX 01 02							
Other staff[45] financed by art. XX 01 04/05							
TOTAL							

8.2.2. Description of tasks deriving from the action

Not applicable.

8.2.3. Sources of human resources (statutory)

(When more than one source is stated, please indicate the number of posts originating from each of the sources)

☐ Posts currently allocated to the management of the programme to be replaced or extended

☐ Posts pre-allocated within the APS/PDB exercise for year n

☐ Posts to be requested in the next APS/PDB procedure

☐ Posts to be redeployed using existing resources within the managing service (internal redeployment)

☐ Posts required for year n although not foreseen in the APS/PDB exercise of the year in question

8.2.4. Other Administrative expenditure included in reference amount (XX 01 04/05 – Expenditure on administrative management)

---

43 Cost of which is NOT covered by the reference amount.

44 Cost of which is NOT covered by the reference amount.

45 Cost of which is included within the reference amount.

EUR million (to 3 decimal places)

Budget line (number and heading)	Year n	Year n+1	Year n+2	Year n+3	Year n+4	Year n+5 and later	TOTAL
1 Technical and administrative assistance (including related staff costs)							
Executive agencies[46]							
Other technical and administrative assistance							
intra muros							
extra muros							
Total Technical and administrative assistance							

8.2.5. Financial cost of human resources and associated costs not included in the reference amount

EUR million (to 3 decimal places)

Type of human resources	2006	2007	2008	2009	2010	2011
Officials and temporary staff (XX 01 01)						
Staff financed by Art XX 01 02 (auxiliary, END, contract staff, etc.) (specify budget line)						
Total cost of human resources and associated costs (NOT in reference amount)						

Calculation–*Reference should be made to Point 8.2.1, if applicable*

[46] Reference should be made to the specific legislative financial statement for the Executive Agency(ies) concerned.

8.2.6 Other administrative expenditure not included in reference amount

EUR million (to 3 decimal places)

	2006	2007	2008	2009	2010	2011	TOTAL
XX 01 02 11 01 – Missions							
XX 01 02 11 02 – Meetings & Conferences							
01 02 11 03 – Compulsory committees (27C730)			0.056	0.0375	0.0375	0.0375	0.168
XX 01 02 11 04 – Studies & consultations							
XX 01 02 11 05 - Information systems							
2 Total Other management expenditure (XX 01 02 11)							
3 Other expenditure of an administrative nature (specify including reference to budget line)							
Total administrative expenditure, other than human resources and associated costs (NOT included in reference amount)			0.056	0.0375	0.0375	0.0375	0.168

Calculation – 3 meetings of a supply chain security representatives committee in the first year. - 2 meetings in subsequent years. Reimbursement of national experts' travel expenses, estimated at 25 times an average of Euro 750/expert.