The National Board of Trade

The National Board of Trade is a governmental agency and the central administrative body in Sweden dealing with foreign trade and trade policy. The Board provides the Government with analyses and recommendations.

Within the framework of the European Union, the Board works for an effective Internal Market, an open trade policy in the EU and a strengthened multilateral trading system within the WTO. The Board also acts as ombudsman for free trade and free movement within the EU as partners of the SOLVIT network. This connects governmental agencies across Europe helping companies and individuals caught between differing regulatory systems.

www.kommers.se
Foreword

The number of security initiatives that exert an influence on international trade has increased continuously after the terrorist attacks on September 11, 2001. The requirements placed on the international supply chain are increasing steadily and it is becoming all the more difficult to obtain an exhaustive picture of the entire system of security requirements. The Swedish Trade Procedures Council (SWEPRO), which is a Swedish forum for cooperation on trade procedures, has established that there is a need for comprehensive information on the security initiatives and the effects they have on international trade. This report, produced by the Swedish National Board of Trade, is a response to this need. The report contains a survey of the most important initiatives, some of the economic studies that have been made on the subject, and a detailed comparison between security initiatives in the USA and EU.

The study shows that the security initiatives continue to expand and it is not easy to provide a clear-cut picture of the ways in which they affect trade, globally or in different regions. As more countries introduce partnership programmes, such as the Authorised Economic Operator programmes, between companies and customs authorities, harmonisation and mutual recognition of the different security initiatives are becoming increasingly important.

Some security initiatives have features of trade facilitation. The ambitions to enhance security and to introduce trade facilitation are thus not necessarily in conflict with each other, but can rather be mutually supportive. In earlier studies, the Board has showed that trade facilitation can provide very substantial benefits, not least in developing countries. The Board would therefore emphasise the importance of utilising this possibility to the full – that the perspective of facilitation can really be integrated in the security initiatives – to enable advantage to be taken of the considerable potential that exists. An increase in globalisation also has the effect that security issues will remain in focus for a long time to come, at the same time as trade facilitation can be essential in order to make full use of the enhanced trade opportunities.

The work at the National Board of Trade has been done in project form in close contact with the organisations included in SWEPRO. The project has been led by Johan Pontén in close cooperation with Sascha Sohlman. The project group has also included Linda Lazslo and Sofia Persson. Fredrik Andersson, Anna Hallam, Ingrid Lindeberg and Lotta Ruokonen from the National Board of Trade have also contributed to the project. The report has been translated from Swedish by Michael Gough at Comtech.

SWEPRO’s working group has included Jan Sjölander (Swedish Trade Council), Bo Svensson (Swedish Trade Federation), Mats Larsson (Swedish Customs Service), Stefan Back and Göran Berg (Swedish International Freight Association), Karin Mannerstedt-Berg (Swedish National Police Board) and Erik Nauclé (H&M Hennes & Mauritz AB). The National Board of Trade would like to take this opportunity to thank them all for their active participation in the work on the study.

Stockholm, January 2008

Lena Johansson

Director-General
Abstract

Since the terrorist attacks on 11 September 2001, the number of initiatives that have the aim of strengthening security in the international supply chain has increased rapidly. The initiatives consist of programmes for partnership between customs authorities and companies, rules for advance communication of data on international shipments, minimum security requirements, standardisation of security management and cooperation between companies. Most of the initiatives have been taken by governments or customs authorities but many international organisations are also active in this field. Initiatives have also been taken by companies that have formalised their cooperation in organisations such as TAPA or BASC.

In addition to providing an overview of existing major security initiatives, the National Board of Trade presents a comparison between the rules applied by the USA and the EU in their respective Customs-Trade partnerships and rules on advance information. The study shows that the Customs-Trade partnership programmes are very similar and that few adjustments will be needed for mutual recognition. The comparison also shows that the advance information systems of the two trade blocks are currently well coordinated with the WCO's Framework of Standards, but that the USA's plans for further data collection will be at odds with the current edition of the Framework. Further harmonisation of IT standards would also contribute to a more efficient trade system.

In the report a brief summary is provided of recent studies on the economic impact of the development of security initiatives and an analysis is presented of ways in which costs are distributed. The costs of security measures should be seen in the light of the possible costs of a terrorist attack and subsequent disruption of the international supply chain. Security is a collective good and, in order to optimise the use of resources to achieve security, international coordination is essential in order to avoid free-riders and sub-optimal investments. Intensified security controls can lead to longer transport times, which have an adverse effect on transaction costs and can distort trade. However, many initiatives have the aim of smoother customs procedures for companies with a good track record and more efficient allocation of customs resources, which have a beneficial effect. Companies participating in partnerships with customs authorities report initial costs for implementation of measures but also benefits such as less theft and smoother customs clearance.

The National Board of Trade concludes that, in order not to jeopardise the benefits of trade facilitation, the formulation of security initiatives needs to include trade facilitation measures. The WCO's Framework is an important tool for this work and efforts should be made to promote harmonisation and standardisation between national rules and programmes. Demands for further data collection and 100 per cent scanning of containers do not promote simplification. Further efforts are also needed in the area of transparency.
## Contents

**FOREWORD** 1  
**ABSTRACT** 2  
**PART A: GREATER FOCUS ON SECURITY IN THE SUPPLY CHAIN – A BACKGROUND** 6  

### 1. GREATER FOCUS ON SECURITY IN THE SUPPLY CHAIN AFTER SEPTEMBER 11 7  
1.1 What will be the effects of the security initiatives? 7  
1.2 This study 8  
1.3 Survey, review and analysis 9  

### 2. WHAT IS SECURITY IN THE SUPPLY CHAIN? 10  
2.1 The supply chain – a network? 10  
2.2 What are the threats? 12  
2.3 Introductory review of the security initiatives 13  
2.4 What are the characteristics of a certification programme? 16  
2.5 Financial aspects of security initiatives 16  

**PART B: SURVEY OF SECURITY INITIATIVES** 18  

### 3. INTERNATIONAL SECURITY STANDARDS 19  
3.1 WCO’s SAFE framework 19  
3.1.1 Cooperation between customs authorities 20  
3.1.2 Divisions of responsibilities through the supply chain 21  
3.1.3 Customs-to-business partnerships – Authorised Economic Operators (AEO) 22  
3.1.4 Trade facilitation 23  
3.1.5 Implementation and links to other programmes 23  
3.1.6 Columbus Capacity Building Programme 24  
3.2 International Ship and Port Facility Security Code (ISPS Code) 25  
3.2.1 Introduction of the ISPS Code in the EU 26  
3.2.2 Costs and effects of the ISPS Code 26  
3.3 International standardisation: ISO/PAS 28000 27  
3.3.1 International standardisation – an overview 27  
3.3.2 ISO and security in the supply chain 27  
3.3.3 Standardisation work at the European level 28  

### 4. SECURITY INITIATIVES IN NORTH AMERICA 29  
4.1 USA 29  
4.1.1 C-TPAT 30  
4.1.2 Container Security Initiative (CSI) 37  
4.1.3 Advance Manifest Regulation (“24-hour rule”) 38  
4.1.4 SAFE Port Act 39
4.1.5 FAST
4.1.6 Importer Self-Assessment (ISA)
4.1.7 Secure Freight Initiative
4.1.8 Operation Safe Commerce – support for research
4.1.9 New legislation on 100 per cent scanning of containers
4.2 Canada
4.2.1 Partnership in Protection (PIP)
4.2.2 Advance Commercial Information

5. SECURITY INITIATIVES IN SOUTH AMERICA
5.1 Business Alliance for Secure Commerce (BASC)
5.1.1 Selection criteria
5.1.2 Application procedure
5.1.3 Security
5.1.4 Members’ points of view

6. SECURITY PROGRAMMES IN EUROPE
6.1 The EU’s Customs Security Programme (CSP)
6.1.1 Authorised Economic Operators (AEO)
6.1.2 Rules for the advance notification of imports and exports
6.2 EU rules for other modes of transport
6.2.1 Special rules for air freight
6.2.2 Special rules for maritime transport and ports
6.2.3 Special rules for land transport and rail transport of dangerous goods
6.2.4 Proposal to enhance supply chain security – Secure Operator
6.3 Sweden: Stairway and StairSec
6.4 Quality assurance in the Netherlands
6.4.1 Dutch Client System
6.4.2 PROTECT
6.5 Cooperation between the USA and EU in security matters

7. SECURITY INITIATIVES IN ASIA AND OCEANIA
7.1 APEC/STAR
7.2 EU – China: Smart and Secure Trade Lane Pilot Project
7.3 Australia
7.3.1 Frontline
7.3.2 Authorised Economic Operator (AEO)
7.4 New Zealand - Secure Exports Scheme
7.5 Singapore – Secure Trade Partnership (STP)
7.6 Jordan – the Golden List Program

8. PRIVATE COOPERATION INITIATIVES
8.1 Transported Asset Protection Association (TAPA)
8.1.1 Exchange of Information/Incident Information Service (IIS)
8.1.2 Freight Suppliers Minimum Security Requirements - FSR
8.1.3 Freight Supplier Minimum Trucking Security Requirements (TSR)
PART C: ANALYSIS

DIFFERENT PERSPECTIVES ON THE SECURITY INITIATIVES

9. WHAT EFFECTS DO THE SECURITY INITIATIVES HAVE ON TRADE?
9.1 The effects of terrorism on the international economy
9.2 Security as a collective good
9.3 How should effective security measures be designed?
9.3.1 Security and trade facilitation
9.3.2 Preventive measures or inspections
9.4 Analysis of the benefits and costs of the security initiatives
9.4.1 Benefits of the security programmes
9.4.2 Costs of security
9.4.3 Who bears the costs of enhanced security?
9.4.4 The consequences of security for competition
9.5 How are developing countries affected?
9.6 Summary and conclusions

10. Finding an analytical tool for the security initiatives
10.1 Supply Chain Security Management
10.2 A comparison between C-TPAT, AEO and WCO
10.2.1 The major certification programmes – a step by step comparison
10.2.2 Conclusions
10.3 Comparison of advance notification rules EU – USA – WCO

11. RISK ANALYSIS OF THREATS TO THE SUPPLY CHAIN

12. SUMMARY AND CONCLUSIONS

REFERENCES
Published sources
Official sources
Non-published sources
Web documents and websites
Interviews and other direct sources

ABBREVIATIONS AND CONCEPTS

INDEX

APPENDIX 1: CSI-PORTS
Part A: Greater focus on security in the supply chain – a background
1 Greater focus on security in the supply chain after September 11

The ever-increasing importance of world trade and the development of the modern production system have made society vulnerable to disruptions in the supply of goods. This is illustrated not least by the fact that for more than twenty-five years an ever-increasing number of industries have organised their production in ways that make them dependent on deliveries from their own factories or sub-contractors located in other parts of the world. Stores in the traditional sense of the term are becoming increasingly unusual. Instead, companies receive a continuous flow of goods that are transported in a meticulously calculated way that ensures that they arrive at exactly the very moment that they shall be used as an input in production. This is known as just-in-time production. Even short disruptions in the supply chain can have considerable financial consequences.

During recent years, a large number of initiatives have been taken that have the aim of enhancing security in the supply chain. The background to this is that the risk of terrorist attacks directed at the supply chain is considered to be high. Even if no such attacks have yet taken place, but have instead mainly targeted private persons and public means of communication, there is no guarantee that what may appear to be a somewhat unrealistic threat today cannot occur in the future. Therefore, transport security has become an important global issue.

Even before September 11 and the attacks against the World Trade Center in New York and the Pentagon in Washington DC, preparations had been made in the USA to heighten security in the supply chain. Very soon after September 11, the American customs presented measures such as C-TPAT (a certification programme), and CSI (a port security initiative). BASC, a South American certification programme, was already in existence prior to September 11.

In the years after 2001 a large number of countries and organisations have presented further security initiatives. Parts of these initiatives are statutory obligations, others are voluntary certification programmes. However, the voluntary programmes can be experienced by companies as essential for trading activities and for maintaining tempo in the supply chain.

Apart from enhanced security, incentives for companies to participate in the initiatives can include the possibility of obtaining smoother customs treatment; requirements made by partners, and pure marketing considerations. No company wishes to see its name associated with a consignment that contains terrorist weapons. On the other hand, being associated with security initiatives can be seen as a sign of professionalism, thereby strengthening the name of the company.

1.1 What will be the effects of the security initiatives?

Comments are now being heard from business organisations which emphasise that the large number of initiatives and the lack of coordination between them constitute a problem. For many companies, security needs on the one hand and demands for efficiency on the other constitute a difficult balancing act from the very outset. Many companies are working seriously with security issues, among other things as a measure to prevent theft, as well as to comply with working environment rules and other regulations and to protect their own personnel. These companies naturally have lower costs when undergoing the certification process and for complying with the security rules introduced by the authorities. However, the challenge for all involved is to find a balance between security requirements and international trade that is as efficient and effective as possible.

Fulfilling the new security requirements that are being established for international trade costs money, both for countries and companies. The amount of these costs and the effect they have on the possibilities available to individual countries and companies to participate in international trade are important questions to which answers are still lacking. The large number of new rules and the requirements associated with the new security initiatives also result in higher costs.
There is a risk that these higher costs will be incompatible with the long-term development of an effective trade system. However, at the same time there are studies that show that there are benefits to be gained from the initiatives, benefits that are principally related to a reduction in the amount of goods that are lost through shrinkage and the professionalization of logistical work.

The fact that it costs money to comply with the rules and agreements has been given attention in other contexts: both the European Commission and the Swedish government have explained, for example, that they wish to reduce the rules and the complexity of procedures in general by twenty-five per cent. For its part the Swedish government has stated that the costs incurred by companies for following the rules should decrease by twenty-five per cent. The Swedish Agency for Economic and Regional Growth (Nutek) has been given the assignment of measuring the costs that arise as a consequence of the legislation. Calculating the costs of the various security rules and other effects that the measures can have entailed is, however, complicated and requires meticulous methods work. Hitherto, few studies have been made and their results are not completely clear-cut.

1.2 This study

In this report the Swedish National Board of Trade describes the different global security initiatives. The intention is primarily to provide an introduction to existing programmes and the ways in which they are constructed. In the first place the report tries to answer the following questions:

- What is the content of the existing programmes?
- What effects have they had on companies and, in turn, on trade?
- Are the measures reasonable in relation to the threats?
- Are facilitation and coordination possible?

In our attempt to answer the questions we will try to define and describe what a supply chain is; provide a model for ways in which work on security in the supply chain can be described and classified into categories; make a brief summary of available studies of the financial consequences of the security initiatives, and discuss how effective the different initiatives can be considered to be.

In this study the National Board of Trade has used a perspective that is based on the ambition to achieve trade facilitation. Trade facilitation is a concept that involves reducing the transaction costs of international trade by simplifying trade procedures. Trade facilitation covers the entire transaction chain from exporter to importer, including transport and payment. However, the focus is often on procedures relating to passage across borders and the authorities involved there. Fundamental principles for trade facilitation are transparency, harmonisation, standardisation and simplification. To achieve trade facilitation in the best possible way, full cooperation is necessary on these principles between authorities and trade and industry, as well as between the different authorities that are involved in the supply chain. See figure 1.1.
Harmonisation of legislation and regulations.

Simplification of administrative processes and documents.

Standardisation of information and requirements and using IT to exchange information efficiently.

Transparency – ensuring that information, requirements and processes for crossing borders are clear and specific and easily accessible for all involved.

Figure 1.1 Principles for trade facilitation. Source: National Board of Trade/SWEPRO

1.3 Survey, review and analysis

This report is based on a survey of the different initiatives. During the survey a large number of organisations and companies have been contacted, an extensive study of available literature has been made, and information has been obtained from the customs and other authorities. The National Board of Trade has not made a survey of attitudes or costs at companies. The report is primarily based on written sources.

The analytical sections contain both the Board’s analyses and reviews of studies made by other organisations. The review of the financial effects of the security initiatives that is given in the analytical section of the report is derived from a review of the literature supplemented by a theoretical analysis made by the National Board of Trade on ways in which the costs are broken down among the operators in the supply chain. Furthermore, the comparison between the EU’s AEO programme, the USA’s C-TPAT initiative and the WCO’s AEO programme is based on a study made by the Cross Border Research Association in Lausanne. In addition to this, a comparison is made between the advance notification rules in the EU and USA, contrasted against the rules in the WCO’s framework. The National Board of Trade’s comparison is also compared with corresponding work done by the WCO. Finally, we reproduce the main features of a study made by OECD on security in intermodal container transports1.

---

1 The movement of goods in the same loading unit or road vehicle, using two or more modes of transport. Containers can easily be moved between trucks, trains and ships.
2 What is security in the supply chain?

The international supply chain is vulnerable since it consists of many different parties which handle large amounts of goods and information and since there are many occasions where goods must be reloaded. Vulnerability is twofold: partly the risk that the supply chain is broken due to a terrorist attack, partly the risk that terrorists use a mode of transport to make an attack. At the same time the economy of countries is also vulnerable since many companies are dependent on the supply chain for their production, and supplies for people in general are dependent on international trade.

Other threats have emerged in parallel with the terrorist threat. Both road transports and maritime transport have been increasingly subjected to hijacking. This threat often comes from inside companies in the form of inside jobs. Also, the interest in preventing smuggling of human beings and drugs has been the major driving force behind the emergence of security initiatives (see, for example, sections on TAPA and BASC).

In this section we try to provide a picture of the ways in which the supply chain works and discuss the threats to it. In addition to this we provide an initial picture of the security initiatives that governments, organisations and companies have produced to meet the threats.

2.1 The supply chain – a network?

In a report commissioned by the European Commission it is stated that there are approximately 4.7 million companies in the EU that are involved in the supply chain, according to data provided by Eurostat.2 The supply chain is also very extensive in volume. In 2005 the volume of goods transported in containers was 114 million TEU (Twenty-foot Equivalent Unit – a standard measure for containers).3

A very large proportion of the transports that are necessary for the production systems of today are made in the form of containers. A container is a reinforced steel box with a double door. It can be modified to transport refrigerated and frozen goods, gases or liquid substances, or specially equipped, for example to transport clothes. Where international trade is concerned, the intermodal container transport chain functions rather like the circulation of blood in the body. The system has proved to be very effective and relatively secure and there are possibly further gains, financial and environmental, to be made by strengthening intermodality and nodes.4

One classic representation of the way goods are moved between producers and consumers is a chain of goods, transports and information – a supply chain. The idea is that a raw material or a product is produced, sold and transported to a company which in turn sells it onwards in the chain. This company can be an importer or a wholesaler, which distributes the good either directly or via further distributors to the final customer. In a chain of this type the parties involved are the original producer, the transporter, the wholesaler/importer, possibly further distributors, the retailer and the final customer. It is also possible to add the financial transactions and the associated exchange of information. A supply chain in which the manufacturer and the purchasing company are in different countries is presented in outline in figure 2.1.

---

4 OECD ECMT (2005).
In actual fact the chain is more complex than this. In the example in figure 2.1 there are a number of participants that have different roles. There is a variety of intermediaries in the logistics sector. The most common roles could be said to be transporters, customs agents and freight forwarders. A freight forwarder can be a type of consultant for the entire transport chain who has his own storage facilities and can also perform customs agent services. If, in addition to this, it is considered that the logistics chain has an information component and a financial component, the chain can be illustrated as in figure 2.2 with more active participants, mainly in the financial components. Moreover, it would appear as if the intermediaries used by importers and exporters vary considerably over time, which increases complexity. To describe a definite supply chain at the time, for example, of a certification process merely provides a picture of the situation at that particular point in time.

An even more complicated picture of the ways in which production and distribution take place today could be a network with many branches. A producer of raw materials sells to many different customers, transports the raw material using different modes of transport, and buys logistical services from different companies. The company that processes the raw materials produces a number of different products of which some can be used as inputs in other industries. These industries, in turn, receive other inputs for their production processes from many different places and then sell their final products to a number of different customers via different distributor and retailer networks in different countries. Moreover, it is conceivable that a company which
further processes a product sells it back to the original company that uses it an input in another product manufactured by the company. The result is a network of relations between different companies and their customers with a large number of participants in the intermediary stage – different logistical companies. One example could be the production of a passenger car. The final assembly of the car takes place in an assembly line production process in which a large number of components must arrive in perfect condition and at the right point in time in order that the car can be assembled as quickly as possible. The outermost limits of the supply chain are from rubber to tyres, glass to windows, steel and aluminium to the coachwork etc. Today, few if any car manufacturers take their components from one and the same country – instead the major producers cooperate over the continents of the world with the development and production of products that can be used as inputs in the production process. In turn the cars are then sold internationally.

For financial reasons most modern companies have chosen to minimise stores and stockholdings. Minimising the amount of capital tied up in non-moving stock has provided a way for both industries and consumer goods companies to reduce their costs. Where the manufacturing industry is concerned, this means that large parts of stock are moving in the supply chain in order to be assembled with other components at exactly the right point in time. The same logic applies to many consumer goods: the stock of the clothes shop is on clothes-hangers in the shop. This is one of the explanations of why the supply chain is so sensitive to breakdowns. Even short disruptions in deliveries can involve considerable costs resulting from production stops, delays in deliveries and breaches of contract or dissatisfied customers.

The trend described above is one part of the rationalisation ambitions that have existed in industry since the end of the 1970s when American and West European industries realised that they had to be able to meet competition from Japanese industry at first and later competition from a large number of other nations. The ideas behind the trend have partly been developed in Japanese companies with flexible production as their guiding principle. At the same time the possibilities of obtaining better control of production and the supply chain as a consequence of IT, and increasing demands for higher returns on capital and for lower amounts of capital to be tied up in stock, have made the professionalization of all logistical activities necessary. Logistics has become strategically important in competition between companies and is no longer a dull but necessary transport and stores operation. It also means that many of the measures described in the security initiatives have already been implemented in the major companies and would have probably have taken place even without a greater terrorist threat. It would probably be difficult to determine the extent to which the security initiatives have speeded up this professionalization, but it would clearly seem to be a combination of two factors.

2.2 What are the threats?

The point of departure of a number of surveys of security in the supply chain is the terrorist attacks on goals in the USA on September 11, 2001. However, it should be borne in mind that there had been earlier attacks in many other contexts. The attack against the World Trade Center in 1993, the attack against an American destroyer, USS Cole, in the year 2000, the activities of the IRA and ETA in Europe, to mention just a few. Many developing countries have also been severely affected. What was new in the attacks in 2001 was that a mode of transport became a weapon that was used by the terrorists. Instead of hijacking aircraft, taking hostages and presenting a list of demands, the terrorists transformed one part of the supply chain into an offensive weapon.

Transport security immediately became a priority issue. It was clear that the terrorist threat was not only directed towards modes of transport but could also transform modes of transport into threats. At the same time it was clear that the effects of the breakdown in the supply chain were extensive. The USA closed its borders for up to three days after September 11. The cost of a breakdown in the supply chain immediately became very obvious.

Analysis of transport security can be divided into infrastructural risks (the form of transport is the goal of the terrorist) and risks arising in the supply chain (the form of transport is the tool for the terrorist).
In addition to this, container traffic in particular could be used to transport weapons for use in another context and by other persons. In brief the threat posed by terrorism can be summarised in three points:

- The threat from the supply chain. Aircraft are used as weapons, containers are used as a mode of transport for bombs or the like.
- The threat against the supply chain: Attacks against ports or airports cause major breakdowns in the supply chain.
- The supply chain is used to support other terrorist activities: Illegal transportation of people in containers (see section on CSI), arms smuggling, and so on.

To these three threats can be added the uncertainty that arises from the very existence of threats. A mere threat to carry out a terrorist attack can result in quite considerable strains on the trade system since it has the effect that the companies involved in the supply chain must plan for this eventuality. This can be seen in, among other things, the reactions to threats that are spread on websites with links, real or claimed, to Al-Qaida. The threats from terrorism should be seen as a political trend in which different terrorist networks have become active and have also gained admirers that imitate them. Police authorities in Europe claim they have averted a number of attacks. It would still appear that no threat has affected the transport chain apart from passanger traffic.

2.3 Introductory review of the security initiatives

The initiatives that have been produced to meet the threats to the supply chain are of different types. There are a large number of parties involved in security matters from different perspectives. The security initiatives can be roughly categorised into those initiated by the state or supranational bodies (EU, WCO), and those that have non-governmental organisations behind them. Furthermore, it can be meaningful to classify the initiatives into those that are compulsory and those that are voluntary. This can be a matter for discussion. In practice, it can be essential for companies to participate in initiatives that are formally voluntary to enable them to achieve a greater degree of efficiency in their trading activities.

A presentation is given below of the most important initiatives. The initiatives that have been selected are primarily those that are directed specifically towards companies. They are presented in more detail in following sections in this report. The aim of the presentation below is to give an initial overview and classification to provide support for further reading.

AEO. The World Customs Organization (WCO). In its Framework of Standards to Secure and Facilitate Global Trade (SAFE), the WCO provides among other things a definition of ways in which companies can become Authorized Economic Operators (AEO) and thereby obtain certain advantages in customs and security controls. The WCO has 171 states as members. Of these states 147 have formally declared that they intend to introduce SAFE.

AEO in the EU. The EU’s rules for a system of Authorised Economic Operators (AEO) entered into force on January 1, 2008. It is a system for the certification of companies that are given certain advantages in customs and security controls.

Advance notification to the USA. Where maritime container traffic to the USA is concerned, information on imports to the USA, together with certain information on the cargo, must be provided 24 hours before the cargo is loaded onboard.

Advance notification to the EU. On July 1, 2009, the EU will introduce rules that have the effect that all imports and exports must be notified in advance to the customs authorities. There are different time limits for different modes of transport.

---

5 The WCO’s Framework of Standards to Secure and Facilitate Global Trade is often abbreviated to SAFE. In the text of this report it is referred to as the WCO’s Framework, the framework or SAFE, if it is not given its full title.
BASC. Business Alliance for Secure Commerce. This is a security initiative initiated by Latin American companies which, in cooperation with the American customs authorities, have drawn up a programme that has considerable similarities to C-TPAT. However, BASC is the older initiative of the two.

C-TPAT. Customs-Trade Partnership Against Terrorism. This is the USA customs authority’s certification programme that is directed towards companies in the supply chain. The companies are certified in respect of security and are given certain advantages in customs procedures and security-related controls. Moreover, certification in C-TPAT is a basis for participation in other programmes.

Frontline. Frontline is Australia’s initiative for voluntary cooperation between the Australian customs authority and companies. It has considerable similarities to the Canadian customs’ PIP programme. Australia has also initiated a programme that is intended to correspond to the WCO’s AEO programme (see below).

IMO/ISPS. International Maritime Organization. The IMO is a UN agency that has drawn up rules for shipping: the International Ship and Port Facility Security Code. The code is divided into part A and B. Part A is mandatory for those countries that have signed the convention. Part B is a recommendation. The EU has also made parts of Part B mandatory through legislation.

ISO. International Organisation for Standardization. ISO develops standards for ways for working with and management of certain company processes related to security. It has also produced technical standards for, among other things, seals for containers.

PIP. Partners in Protection. This is the Canadian customs authority’s certification programme for companies. The objective is to reduce smuggling and thefts and also to combat terrorism. It has been upgraded in order to make it more similar to the USA’s C-TPAT and mutual recognition could be achieved.

Stairway® is the Swedish customs certification programme for companies. It started as a programme to simplify rules. A security module, StairSec®, has been added.

Security rules for air freight. In the air transport sector there is a system under which freight forwarders are certified and consignors are designated as known consignors.

TAPA. The Technology Asset Protection Association. This is a global association of companies that contributes to the exchange of information between companies and authorities and which works with security standards, mainly for road transports of high value goods.

As can be seen from table 2.1 below, many of the initiatives directed towards companies are voluntary. However, it is relevant to ask whether companies that have extensive trade relations with a country which has introduced security initiatives produced by its customs authority can realistically refrain from participating in the initiatives in the long-term. In other words C-TPAT and the different AEO programmes are on a sliding scale. The ISPS code is also difficult to classify in a clear-cut way. Part A as mentioned above is mandatory legislation in those countries that have adopted it while Part B is, in principle, voluntary. BASC is a non-governmental organisation with voluntary membership but the initiative has been drawn up in cooperation with the customs authorities in the USA. TAPA has a clearer role as both a private and voluntary initiative. The technical standards of the ISO system have a special position since they can sometimes have the form of an instruction on ways in which companies or organisations shall comply with legislation; sometimes they merely provide business guidance, and sometimes they are referred to directly in the text of laws.

<table>
<thead>
<tr>
<th>Legal requirement</th>
<th>Voluntary</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>C-TPAT, PIP, Frontline, Stairsec AEO (EU, WCO)</td>
</tr>
<tr>
<td>Private</td>
<td>ISO 28000, BASC, TAPA</td>
</tr>
</tbody>
</table>

Table 2.1 A tentative classification of the security initiatives on the basis of the legal requirements and forms of ownership
The breakdown above provides, however, only part of the picture. The security initiatives also refer to different parts of the supply chain and allocate responsibilities to different parties. This makes an analysis of the initiatives difficult. For example, it is not possible to compare the rules for advance notification with programmes that certify that companies are working in satisfactory manner with security and compliance with customs rules. One way to understand the initiatives better is to classify them on the basis of the organisation(s) responsible for them and their focus.

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Focus</th>
<th>Examples of initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs authority or other government authority</td>
<td>Certification customs – companies</td>
<td>C-TPAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AEO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIP</td>
</tr>
<tr>
<td>State or supranational body (EU, UN)</td>
<td>Information requirements</td>
<td>Advance notification</td>
</tr>
<tr>
<td>State or supranational body (EU, UN)</td>
<td>Minimum levels for controls and protective measures</td>
<td>ISPS code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100% scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Air freight rules EU/USA</td>
</tr>
<tr>
<td>Private companies</td>
<td>Fewer thefts</td>
<td>TAPA</td>
</tr>
<tr>
<td></td>
<td>Less smuggling</td>
<td>BASC</td>
</tr>
<tr>
<td>Standardisation bodies</td>
<td>Application of certification programmes</td>
<td>ISO 28000</td>
</tr>
</tbody>
</table>

Table 2.2 A survey of security initiatives broken down by the party responsible for the initiative and its underlying focus

There is a relatively large number of certification programmes and they can increase in number if the WCO’s Framework is followed by a large number of the organisation’s member states (see section on WCO). If initiatives for programmes have not been taken at government level, it is the customs authorities themselves that have seen closer cooperation with companies as a method of exerting better control and of being able to collect information that enables them to use their resources in a more optimal way. The different initiatives that regulate the submission of information by companies are often linked to certification programmes and to risk analyses made by customs authorities when selecting the focus of their controls. The rules for the submission of information are mostly binding. At the same time there is a desire on the part of governments and states to guarantee a minimum level in certain fields, or to establish rules for ways in which controls shall be performed. This is the case, for example, with the rules for the treatment of air freight or that part of the ISPS code that is binding. Private companies have also combined efforts to share experience and knowledge and to draw up strategies for security. This is the case with both BASC and TAPA which have come into being since companies have wanted to reduce the frequency of smuggling or theft.

The controls which can be avoided through certification are primarily security controls. This is a case of inspections of documents, in which a risk assessment is made. The assessment constitutes the basis of a decision whether the customs authorities shall proceed with checks of radioactivity or inspections with x-ray or gamma ray technology, so-called Non-Intrusive Inspections (NII). Thereafter, physical inspections of the contents of a container can also be considered. The delays associated with this type of control can be lengthy. In addition to this there are checks of customs documentation, imports of prohibited substances, food controls etc, which are not normally included under these programmes.
The Swedish Customs is of the opinion that some of the controls referring to compliance with the rules can also be included amongst the controls which certification can reduce in order to make the programmes more attractive.

Standardisation bodies have also seen the necessity of becoming engaged in security problems. This applies to both technical standards used for equipment in the supply chain and management systems which provide standards for ways in which companies should work with different security matters or even ways in which they should implement certain certification programmes. In the analytical section of this report there is an in-depth discussion of this classification.

2.4 What are the characteristics of a certification programme?

Many of the security initiatives described in this report are certification programmes. The principle is that the customs authorities in a country enter into partnership with companies and offer them reductions in security controls and other controls in return for which the companies continuously document that they are working with security matters in the prescribed way. In many of the certification programmes there are different levels at which a company, depending on the closeness of its relations with the customs authorities, is granted reductions in controls and other benefits. Examples of programmes of this type are, as mentioned above, C-TPAT, PIP, the Stairway together with StairSec, and the EU’s AEO programme. Certification programmes can offer an opportunity for the legislator to deal with the organisations and companies that are not easy to reach by granting permits. For ports and airports, which are relatively small in number, the authorities grant permits and prescribe minimum rules for security work. Certification programmes can be an efficient way of working with companies since there are too many of them to be rapidly controlled.

In a study made in 2006, researchers at the Cross Border Research Association in Lausanne present a framework for analysis of security initiatives for the supply chain. They state that all security measures work towards five different goals:

- Facility Management: securing premises where goods are handled, stored and loaded.
- Cargo Management: protecting the goods during all stages of their transportation.
- Human Resources Management: ensuring that the background of all personnel is checked and that they are reliable and aware of risks.
- Information and Communication Management: protecting important data and using information as a tool for tracing illegal activities and shortcomings in security.
- Business Network and Company Management Systems: including security in the internal and external structure of the organisation and in the company’s business systems.

Gutiérrez and Hinsa say that these components, in combination, form a system for Supply Chain Management. The model appears to be most suitable for certification programmes even if other security initiatives can be included in it. It does not bring up the aspect of simplification of rules and reductions of controls as a result of certain security procedures. In the analysis section of this report, this model is discussed further and the analysis made by Gutiérrez and Hintsa is used to describe some certification programmes.

2.5 Financial aspects of security initiatives

The financial aspects of the security initiatives are discussed in more detail in chapter 9 of this report. For a deeper understanding of the description of the security initiatives that follows in

---

Part B below, it can be of interest to be aware at this stage of some of the issues that are treated in more detail in chapter 9.

One central problem with security in the international supply chain is that it constitutes a collective benefit and as such requires cooperation and coordination in order to function effectively. A lack of coordination can lead to countries investing in national security at the expense of cooperation in global security. This can lead to ineffective solutions, since coordinated work on security is, in all likelihood, more cost-effective. In addition, cooperation would minimise the risks of disruptions in the flow of goods. However, to be able to coordinate security in the international supply chain, harmonised and compatible systems are essential, both for customs work and for the exchange of information.

The costs that can arise with the introduction of stricter rules for security are of different types. Depending on the type of initiative, the parties involved in the supply chain have, as a rule, an initial cost linked to the implementation of the initiative, such as the introduction of new routines, the acquisition of new equipment and the certification fee itself. After these measures have been implemented, there are still the regular costs of work on security.

Heightened security requirements can also lead to an increase in transaction costs, which can comprise more complicated customs clearance procedures and longer waiting times at ports and terminals. After the attacks against the USA on September 11, 2001, there was an increase in transaction costs in international trade: among other things transport times became longer and more irregular. From the financial perspective, security-related costs are often compared to the duty on a product. A study presented in chapter 9 indicates that each day a product is being transported by sea corresponds to a duty of 0.8 per cent on the value of the product. The question of whether intensified security requirements in the supply chain lead to lengthier transport times is thus extremely relevant, also in view of the fact that trade volumes generally show great sensitivity to the costs of transport. It would consequently appear that there is a relationship between transport times and trade volumes.

In general it can be said that the costs relating to a potential terrorist attack are extremely high. On the other hand it is difficult to measure the direct benefits of enhanced security. The problem lies in the very nature of the benefits since it is not possible to determine the costs that arise from a breach of security that never occurs.

In addition to the benefits of avoiding being the subject of a terrorist attack, there are benefits for companies, primarily from the certification programmes, which can be said to be positive side-effects or spinoff effects. The main spinoff effect must be considered to be the possibility available to companies to continue operations during disruptive incidents. In addition to this, there are benefits arising from a reduction in the number of controls, better relations with the customs authorities, a reduction in thefts and shrinkage, and the possibility of having lower insurance premiums. Moreover, the guidelines in the certification programmes lead to a greater degree of professionalism in the logistics chain which can be an advantage for certain companies.
Part B: Survey of security initiatives
3 International security standards

There are a large number of organisations that produce technical and other standards, nationally, regionally and internationally. The need of standardisation first became apparent in the technical field. Standards are usually voluntary or based upon agreements between states which, in turn, can use them to draw up mandatory rules. It is not uncommon for references to be made to standards in legislation. Likewise, standards can refer to legislation and show ways in which legislation expressed in general terms can be implemented.

Currently there are three major international security standards, all of which have been drawn up to enhance security in the supply chain at the global level: The World Customs Organisation’s Framework of Standards to Secure and Facilitate Global Trade (WCO’s SAFE framework); the International Ship and Port Facility Security Code (ISPS Code), and ISO/PAS 28000.

Even if the ISPS code is the most highly developed and the most widely disseminated programme, the WCO’s SAFE framework is the programme that has the greatest ambitions, since it is applicable to all modes of transport and includes both company certification and highly developed cooperation between national customs authorities. Moreover, the WCO’s SAFE framework is the programme that many countries are making preparations to implement. This is apparent when examining the security initiatives in the section on Asia and Oceania or when taking the statement made by the American customs authority into consideration (see chapter 4 on the USA).

These programmes differ in several ways. While both the ISPS Code and WCO’s SAFE framework are programmes that involve government agencies, ISO/PAS 28000 is primarily a certification programme for non-governmental organisations and companies. The ISPS Code refers exclusively to security in maritime transportation, while the other two also cover other modes of transport.

3.1 WCO’s SAFE framework

The World Customs Organization was established in 1952 under the name Customs Co-operation Council. Its mission is to improve the effectiveness of customs administrations by, among other things, creating international instruments for the harmonisation of customs systems and by effective communication between its member states. With the entry of Laos in January 2007 the WCO now has 171 members.

The year 2005 saw the publication of the WCO’s Framework of Standards to Secure and Facilitate Global Trade (SAFE). In common with other security programmes that are described in this report, this is an initiative that is intended to improve security in the supply chain and, at the same time, to facilitate international trade. The WCO’s SAFE framework emphasises the unique opportunities available to customs authorities to improve security in international trade. However, in order to ensure that the work of the customs authorities does not have an inhibiting effect on world trade, it is necessary, according to the WCO, to have a set of international customs standards that do not counteract or duplicate other requirements made in cooperation between states. The WCO’s large number of member states, which represent 98 per cent of world trade, is used as an argument that the WCO is the obvious platform for a global framework of this type.

The framework is one of the most ambitious initiatives for security in the supply chain, since it includes all member states in the WCO and is based on cooperation both between different customs authorities and between companies and customs authorities. Moreover, the framework also applies to all modes of transport.

Objectives and principles

According to the WCO, SAFE is intended to establish standards that create security in the supply

---

7 World Customs Organization (2005).
8 http://www.wcoomd.org/home_about_us.htm
chain in order to create confidence and predictability. Security shall be made possible for all modes of transport in the supply chain. Furthermore, the role and function of the customs authorities shall be strengthened through SAFE, as well as cooperation between customs authorities to enable them to enhance their prospects of identifying high risk consignments. Another important component is to strengthen cooperation between customs authorities and companies, while promoting smooth flows of goods through secure supply chains.

Three target groups have been identified that will derive benefits from SAFE: states/governments, customs authorities and companies. The economic growth and development of states and governments will be strengthened since SAFE secures and simplifies international trade and, at the same time, combats terrorism. Extended and enhanced cooperation between customs authorities will have the effect that they can make inspections earlier in the supply chain and, in addition, allocate their resources more effectively. Where companies are concerned, the international trade facilitation will have the effect that it is easier to move goods between countries, and Authorised Economic Operators (AEO) will find that their goods are cleared more rapidly by the customs which, in turn, will produce savings in the form of reductions in time and costs.

SAFE is based on four core elements which are intended to permeate the work of improving security in the supply chain:

**Advance electronic information:** SAFE has been formulated in such a way that it harmonises the elements of data required in electronic advance information on imports, exports and transit shipments.

**Risk management:** each country participating in SAFE undertakes to introduce a consistent risk management approach that addresses threats to security.

**Outbound inspection:** in line with the importing country’s request and based on a comparable risk targeting method, the exporting country shall perform an outbound inspection of high risk containers and cargo, preferably with equipment that does not require the cargo to be physically opened, for example large-scale X-ray machines and radiation detectors.

**Business partnership:** SAFE defines benefits that customs authorities shall offer businesses that meet minimal supply chain security as well as standards and best practices.

SAFE consists of 17 security standards broken down into two pillars: customs to customs network arrangements and customs to business partnerships. This structure follows the WCO’s existing security and facilitation measures and programmes that have been developed by the member states.

### 3.1.1 Cooperation between customs authorities

The main idea behind cooperation between customs authorities is that information on cargo shall be provided as early as possible in the supply chain to ensure that high risk containers and other high risk cargo can be identified prior to their arrival in the importing country. This pillar includes, among other things, requirements that customs authorities are given sufficient powers that enable them to demand electronic information from the exporter and transporter in advance in order to perform risk analyses. The customs authority in the exporting country should, at the request of the importing country, implement outbound security inspections. When the customs authority in an importing country suspects that a container or any other form of goods may constitute a security risk, it can request that the customs authority in the exporting country makes an inspection, preferably before the goods are loaded.

This is an area which can prove to be problematical since requirements of this type are contrary to the export legislation of certain countries. Where the USA is concerned, the country’s export legislation prohibits the submission of information to foreign governments which its automated export system has collected from the export declarations of shipping companies. In addition, this system requires customs authorities to introduce computerised customs systems that include the exchange of electronic information on exports and imports, which has led to concern about
expensive revisions of information handling procedures in many countries.\(^9\)

The customs authorities shall establish risk management systems in order to identify potential high risk containers. The systems should include a mechanism for the approval of analyses of threats. The customs authorities shall also cooperate with other authorities in order to make security assessments of the transport of goods in the international supply chain. Other requirements include checks on and training of personnel and compatible mechanisms for the exchange of information. The WCO’s standards for cooperation between customs authorities are summarised in fact box 3.1 below.

### Fact box 3.1 WCO’s standards for cooperation between customs authorities

#### 3.1.2 Divisions of responsibilities through the supply chain

The WCO’s SAFE framework specifies the party that bears the responsibility for goods transported in containers from the time when they are packed to the place where they are unloaded. Certain principles and areas of responsibility are common to all operators involved in the entire cycle of a container transport. All operators that handle a container in one way or

---

\(^9\) This issue has often come up in the Columbus programme (see section below). According to the WCO these problems have proved to be fewer than expected and the greatest problem is not a lack of IT systems and equipment, but rather the systematic underutilisation of existing systems.
another share this responsibility. The areas of responsibility include protection of physical goods against tampering, theft and damage. Furthermore, authorities shall receive timely and relevant information to enable them to perform their security inspections. Moreover, information relating to goods shall be protected from tampering and unauthorised access. This applies to the period of time before, during and after an operator has had custody of the goods.

Where custody of goods in the supply chain is concerned, the seal is of central importance. Security seals shall be inspected by the recipient party every time the custody of the goods is passed on. Inspection shall include visual checks of any signs of tampering, comparison of the identity number of the seal with cargo documentation, and noting the inspection in the appropriate documentation in the correct way.

3.1.3 Customs-to-business partnerships – Authorised Economic Operators (AEO)

Both member states of the WCO and the private trade sector recognise the importance of securing the supply chain, and facilitating the flow of international trade. Cooperation between customs authorities and companies has been designed to achieve this goal and under this pillar demands are made, among other things, of a partnership between an AEO company and a customs authority being strengthened by business partners of the AEO company certifying in writing that they intend to follow the security standards in SAFE. Requirements are laid down that an AEO shall incorporate predetermined best practices in respect of securing buildings and interior and exterior perimeters, identification procedures for its employees and visitors, protection of sensitive information, personnel security, reporting procedures for transport information, and training in security for its personnel.

In this pillar, requirements are also stipulated in respect of the use and documentation of security seals, communication routines in emergencies, and streamlining of customs clearance procedures. The WCO’s standards for cooperation between customs authorities and companies are listed in fact box 3.2 below.

**Fact box 3.2 WCO’s standards for cooperation between customs authorities and companies**

- Partnership
- Security
- Authorisation
- Technology
- Communication
- Facilitation

The WCO has detailed requirements for companies that wish to obtain AEO status. An AEO is defined as a party involved in the international movement of goods that complies with the WCO’s standards or equivalent supply chain security standards. Authorised operators can be, for example, manufacturers, importers, exporters, brokers, carriers, consolidators, ports, airports, terminal operators, owners of storage premises and distributors. To avoid a situation in which small and medium-size companies in particular are negatively affected by complicated procedures that may be necessary for large companies, the WCO advocates flexible application of AEO status. If the requirements can be secured in a more cost-effective way for a small or medium-size company, this method shall be used. One example of an aspect of this type is detailed checks of personnel which, in a smaller company, can be replaced by the existence of a personal relationship between the owner and all the employees. The requirements for becoming an Authorised Economic Operator are listed in broad outline in fact box 3.3 below.
3.1.4 Trade facilitation

In addition to security work, SAFE is also designed to facilitate international trade. This part of the framework is based on the revised Kyoto Convention, which was drawn up to facilitate international trade. The aim of the revised Convention is, among other things, to eliminate differences between different customs authorities which can act as a barrier to international trade. The importance of risk analysis as an instrument for security in trade is emphasised in the Kyoto Convention and, in order to avoid unnecessary trade barriers, security measures shall be kept to a minimum.

3.1.5 Implementation and links to other programmes

The concept of Authorised Economic Operators is, as mentioned above, of central importance for security in the supply chain. At the present time it is the subject of discussion among various parties that wish to improve security bilaterally, which is a point of departure for mutual recognition. The EU’s AEO programme is to be fully compatible with the AEO programme in SAFE, and the European Commission has participated actively in the development of SAFE. The WCO’s AEO model is designed to cover both trade facilitation and security and has its point of departure in recognition between countries. Since the EU’s AEO programme is based on a model in which the AEO concept is split into two variants, AEO – Customs Simplification and AEO – Security and Safety, or a combination of both of them, it is only the latter combined variant that is compatible with the WCO’s AEO programme. In this context the WCO emphasises the importance of having an integrated, standardised model for recognition of AEOs and controls.

It is not only the AEO programme that functions as a link to other initiatives for security in the supply chain. In June 2002 the WCO’s member states decided unanimously that ports in all member states could start programmes based on the principles contained in the Container Security Initiative (CSI). There are also strong links between the WCO’s work and the Customs-Trade Partnership Against Terrorism (C-TPAT). The American customs authority participates in the WCO’s Task Force on Supply Chain Security which, in 2002, was given the mandate to develop guidelines for partnership between companies and customs authorities. The fact that the USA is a strong force behind the development of SAFE is apparent if the way in which the framework has been built up is studied. It is based on several principal elements in the programmes that the American Customs have created, in particular C-TPAT and CSI. The principal difference between SAFE and the American programmes is that SAFE requires standards for both exports and imports, while the American programmes only lay down security requirements for imports.

Fact box 3.3 Main points in the WCO’s programme for Authorised Economic Operators (AEO) in SAFE

- Demonstrated compliance with customs’ requirements
- Satisfactory system for management of commercial records
- Financial viability
- Consultation, cooperation and communication
- Education, training and awareness
- Information exchange, access and confidentiality
- Cargo security
- Conveyance security
- Premises security
- Personnel security
- Trading partner security
- Crisis management and incident recovery
- Measurement, analyses and improvement

It is possible to make changes to SAFE in regular three-year cycles unless the changes relate to extraordinary events that necessitate an urgent change. The proposal on advance notification of further data in connection with imports to the USA (SAFE Port Act’s 10+2) is not compatible with SAFE. However, since it has not yet gone through the entire referral procedure in the USA and become law, the USA has not yet requested a change to SAFE.

To enable the introduction of SAFE to take place smoothly and be adapted to the prevailing situation in each member state, it shall be possible for the states to introduce the programme at different levels. This means that the components of SAFE and their treatment will vary from country to country.

One factor of central importance where cooperation between customs authorities and companies is concerned is the costs that SAFE leads to for small and medium-size companies, particularly in developing countries. A number of working groups in the WCO have been formed in cooperation between trade and industry to ensure that these companies’ interests are monitored in the work on SAFE. In this discussion it is important to make a distinction between programmes that have been initiated for security and crime-prevention reasons and then extended to include measures related to trade facilitation, and those that have been developed to create more effective processes and facilitation for trade and industry and then extended with security and crime prevention modules and elements. According to information received, large companies have greater advantages than small companies in the former category.

3.1.6 Columbus Capacity Building Programme

In view of the global character of the WCO, the question arises whether all member states will be able to implement SAFE in its entirety. There is a clear risk that countries which lack capacity, in the form of both infrastructure and administrative capacity, will not be able to fulfil SAFE’s requirements in respect of security measures. This could have the effect that the participation of poor countries in international trade could be made difficult as a consequence of SAFE. To rectify this problem the customs authorities in the USA, Canada, Australia, the EU and Japan have undertaken to offer help to developing countries that show the political will to implement SAFE but lack the means to do so. Each country shall have an individual implementation plan. However, the WCO is also working with the regional introduction of SAFE. For example, the East African Community, SACU, ECOWAS and ASEAN shall cooperate to harmonise the introduction of SAFE.

To enable the member states to introduce SAFE, the WCO started the Columbus Programme in 2006. It is a programme containing three phases:

- Needs assessment: a mission which results in a diagnostic report that contains the needs analysis and recommendations on ways in which any shortcomings can be rectified.
- Implementation: administrations that have been the subject of a diagnosis shall prepare plans of action that are based on the strategic report presented in phase one.
- Monitoring: the administrations shall present a SAFE control report. In September 2007 diagnostic missions had been finalised in 109 member administrations and 35 member states were in the implementation phase.

The WCO underlines in a report that scanning containers is a useful instrument to enhance security in the supply chain, but emphasises at the same time the importance of installing Non-Intrusive Inspection (NII) equipment with care. If a system of this type is to function effectively it is necessary, according to the WCO, that the infrastructure for risk assessment is in place first. This also has the effect that it is necessary that the customs receive information about cargo in advance so that high risk containers can be selected for scanning. Furthermore, the WCO

12 World Customs Organization (2007).
13 NII equipment usually consists of equipment for X-ray, gamma-ray scanning and measurement of radioactivity.
expresses concern that NII equipment is acquired without a correct needs analysis and that some authorities feel under pressure to install equipment for scanning, which is a source of large amounts of money for the manufacturers of these machines.

Since more than 100 countries have now completed the diagnostic phase, a great deal of focus is on the challenges that will be faced in the second phase: implementation. A large number of countries will need help to introduce SAFE, both from the WCO and from donor institutions. In order to receive help from the WCO it is necessary that these countries show the political will to modernise, that they have produced a plan of action and acquired financing for this plan, and that the breakdown between regions is in balance.

### 3.2 International Ship and Port Facility Security Code (ISPS Code)

The International Maritime Organization (IMO) was established in 1948 in Geneva. It is an agency in the UN system. Its main mission is to develop and maintain international rules for shipping which include safety, environmental concerns, legal matters, technical cooperation and efficiency in shipping. The IMO has 167 member states at the present time. The basic foundation of the IMO’s work is the Safety of Life at Sea Convention (SOLAS), which is the most important treaty addressing maritime safety, the first version of which was issued as a response to the Titanic disaster of 1912. Since then several new versions have been adopted, the most recent in 1974. SOLAS is an extensive set of regulations for safety-related issues, for example carriage of dangerous goods, radio communications, life-saving appliances and fire safety provisions for all ships.

After the terrorist attacks on September 11, 2001, the members of the IMO agreed to develop security measures for ships and ports. The result was the International Ship and Port Facility Code (ISPS Code) which lays down requirements in respect of maritime security and recommendations on ways in which these requirements shall be met. The ISPS code, which was included as an amendment to SOLAS, was introduced in July 2004 and in August of the same year 89.5 per cent of 9,000 ports and more than 90 per cent of all ships had been approved in accordance with the Code. According to the IMO14, the introduction of the code took place unevenly between different regions. Africa and countries in the former Soviet Union and in Eastern Europe were slow in introducing the new security rules.

The goal of the ISPS Code is, according to the IMO, to establish an international framework for cooperation between governments, government agencies, local administrations, and shipping and port industries. This framework is intended to facilitate the detection and analysis of threats to security and the introduction of preventive measures to meet security incidents that affect ships or port facilities used in international trade. With the aid of the Code the roles and responsibilities of all parties shall be defined, at both national and international level, for ensuring maritime security. It shall ensure the early and efficient collection and exchange of information related to security, and provide a methodology for security assessments to enable suitable and proportional measures to be taken as a reaction to changes in needs of security.

These goals shall be achieved through the appointment of suitable security personnel on each ship and at each port office and shipping company to prepare and introduce security plans.

The ISPS code applies to

1. The following types of ships on international voyages:
   - Passenger ships, including high-speed passenger craft
   - Cargo ships, including high-speed craft, of 500 gross tonnage and upwards
   - Mobile off-shore drilling units
2. Port facilities that serve these ships.

---

The ISPS Code is in two parts. Part A includes mandatory measures such as the appointment of security personnel and the drawing up of security plans. Part B includes guidelines and recommendations on ways in which security plans for ships and port facilities should be prepared.

The ISPS Code includes security measures at three levels: security level one is the level at which ships and ports work in normal situations. Where security for ships is concerned, routines shall be introduced for, among other things, access to the ship, control of persons that go onboard including their baggage, and the surveillance of decks and areas in immediate proximity of the ship. Whenever there is a high risk for a security incident, security level two is introduced and the above routines are intensified. Security level three, which is introduced in exceptional cases where there is an imminent risk of a security incident, leads to a further intensification of the routines. The third security level shall only be applied as long as there is an immediate risk of a security incident and, as soon as this risk diminishes, the level shall be lowered. Part B contains detailed regulations on the security routines that shall be introduced when the security level is changed. Under security level three, access to the ship shall only be permitted at one point which shall be under strict surveillance.

3.2.1 Introduction of the ISPS Code in the EU

Before the ISPS Code came into effect on 1 July 2004, it was decided that its implementation should be standardised within the EU. Therefore, on 31 March 2004, EC Regulation 725/2004 was adopted. This had the effect that part A of the ISPS Code became applicable with direct effect in the EU member states. The same applies to certain parts of Part B.

One idea behind the decision to make certain measures in Part B of the ISPS Code mandatory in EC Regulation 725/2004 was that differing opinions about - and differing measures linked to - maritime security could threaten the security of the EU. However, it was also feared that the character of Part B – recommendations - could lead to differing interpretations which, in turn, could lead to inequalities in competition.

This approach has led to certain critical reactions. Firstly, differences in the implementation by member states could be the same that could arise between all the other parties that had adopted SOLAS. Furthermore, these differences could allow fine adjustment of security measures on the basis of each specific situation in each state. Secondly, the critics maintain that differences in implementation have already arisen among member states.

3.2.2 Costs and effects of the ISPS Code

In a report from UNCTAD, a study was presented of costs related to the introduction of the ISPS code incurred by ports around the world. This analysis showed that costs are very much related to the size of the port. Initial costs relating to the ISPS Code over a five-year period correspond on average to one per cent of the ports’ income. This figure is higher for small ports than for large ports, even if the difference is only 0.4 per cent. The annual running cost corresponds on average to two per cent of the income. For small ports this figure is three per cent and for large ports one per cent. When calculated on the basis of a twenty foot container (TEU – Twenty-foot Equivalent Units) the differences are greater: for small ports the initial cost of ISPS over a five-year period is on average USD 2.30 per container, while for large ports the cost is USD 0.80 per container. The annual operating cost for small and large ports is USD 2.50 and USD 1.60 respectively.

UNCTAD also asked these port offices how they perceived the overall effect of the ISPS code. Sixty-four per cent responded that the implementation of ISPS had had a positive effect, for example since it offered a mechanism to standardise security in all parts of the port. Twenty-four per cent were of the opinion that, without exception, it had had a negative effect. Costly and

15 Anyanova (2007).
arduous introductory activities and serious disruptions of daily business activities were presented as problem areas. Twelve per cent were of the opinion that it had had a limited effect since investments to counteract theft and other criminal activities had already been made before the introduction of the ISPS Code.

When representatives of governments were given the same question, 82 per cent responded that the introduction of the ISPS Code had, without exception, been positive; 15 per cent responded negatively and only three per cent responded that it had had a limited effect.

3.3 International standardisation: ISO/PAS 28000

3.3.1 International standardisation – an overview

At the international level, standardisation work is mainly pursued by a non-governmental organisation: the International Organization for Standardization. National standardisation institutes are linked to the ISO through agreements. Membership is national which has the effect that only one organisation in each member state is permitted to be a member. Its work primarily concerns technical areas, but quality assurance and environmental work have been taken up. The quality assurance standard ISO 9000, together with its sub-groups, and environmental assurance standard ISO 14000 have had a considerable impact since the 1980s when quality work became a priority area in industrial production in Western Europe and the USA.

Standardisation in the EU and EFTA is pursued primarily through the European Committee for Standardization (CEN). There is an agreement under which the national standardisation organisations undertake to dispense with national standards in favour of CEN standards when they are approved. If there are deviations in national standards that are motivated by national legislation, CEN shall be informed. However, deviations are only permitted in those fields that are not already harmonised in the EU.

3.3.2 ISO and security in the supply chain

ISO produces standards through the work of its technical committees. A standard is adopted if at least 75 per cent of the member organisations adopt it. In cases where the ISO sees that it is particularly urgent to produce a standard, the technical experts in a working group can produce a standard that is then approved if it is adopted by at least 50 per cent of the member organisations that are represented on the technical committee. These ISO/PAS – Publicly Available Specifications – can later be upgraded to regular standards.

In 2005, ISO adopted ISO/PAS 28000, Specification for security management systems for the supply chain, which is a standard to enhance security in the supply chain. The idea behind this standard is to facilitate better controls of flows of transport, to combat smuggling, and to meet the threats of piracy and terrorism, and to create a secure management of the international supply chain.

ISO/PAS 28000 is a security standard based on the so-called Plan-Do-Check-Act method which the ISO explains in the following way:

- **Plan**: to specify necessary goals and procedures to achieve results, in line with the organisation’s security policy
- **Do**: to introduce the routines in question
- **Check**: to check and measure procedures on the basis of the security policy, goals and objectives
- **Act**: to continuously improve security management systems.
The system proposed in ISO/PAS 28000 includes aspects such as financing, production, information management and packing, storing and transport of goods. It shall be possible to implement by organisations of all sizes, form small-scale to multinational, that wish to:

- Establish, implement, maintain and improve a security management system;
- Assure compliance with stated security management policy;
- Demonstrate such compliance to others;
- Seek certification/registration of its security management system by an accredited third party certification body; or
- Make a self-determination and self-declaration on compliance with ISO/PAS 28000.

The management of an organisation shall draw up and adopt a comprehensive security policy. This policy shall be adapted to ensure that it corresponds with the organisation’s other policies. It shall also be adapted to identified threats against the organisation. The policy shall be documented and published and all members of the organisation shall be informed about it. The organisation can choose to have a detailed security policy for internal use which can be confidential and a brief, non-confidential version that parties outside the organisation can be given.

ISO/PAS 28000 has considerable similarities to the environmental management system ISO 14000. It is a system which primarily focuses on ways in which management and control systems can be developed. No detailed guidelines are provided for ways in which different security solutions in the physical environment should be designed. The standard is intended to provide guidance to ways in which the entire flow shall be secured and, in the pilot programme being implemented by Technical Committee 8 (TC8), a number of transport routes are being studied.

Furthermore, ISO has published an in-depth Draft International Standard ISO DIS/28004 and ISO 28003 which contain principles requirements for bodies that wish to be entitled to implement ISO certifications. Furthermore, there are a number of other standards, published or under production, that touch upon security in the supply chain in various ways. These are ISO/PAS 20858 which concerns implementation of the ISPS Code, ISO 17712 on mechanical seals, the ISO 18000 series on Radio Frequency Identification (RFID) (see section on CSI), the ISO 9735 series on EDI, and others.

3.3.3 Standardisation work at the European level

Standardisation in the EU and EFTA is pursued, as mentioned above, mainly by the European Committee for Standardisation (CEN). Where security in the supply chain is concerned, CEN commissioned a working group on Supply Chain Security under Working group 161 “Protection and Security of the Citizen” to draw up a report on the need of standardisation. In the report the expert group draws the conclusion that there is a great need of standardisation in this field. At the same time CEN says that it intends to collaborate with ISO and examine whether it is possible to harmonise and simplify existing standards, procedures or rules. At the time of writing, CEN is in the process of establishing a Task Force on the subject and recruiting a technical expert in the field.
4. Security Initiatives in North America

4.1 USA

The terrorist attacks of September 11, 2001, against New York and Washington were the starting point of a greater focus on security in the transport chain. Immediately after the terrorist attacks, air traffic to and from the USA came to a halt, the border with Mexico was closed completely for a short period of time, and the border crossing points between the USA and Canada were affected by long queues with resultant delays in the transport of goods. Many industries in the USA that are dependent on regular supplies for the smooth running of their just-in-time production activities had to stop production for short periods of time.

The American economy is dependent on foreign trade to a relatively small degree: in 2006 imports of goods and services corresponded to approximately 17 per cent of GNP. However, USA trade is of decisive importance for the world economy and is large in absolute figures. The value of all exports in 2006 was approximately USD 1 445 billion, and of all imports approximately USD 2 200 billion (goods and services).18 Many countries are dependent on their exports to the USA and the flow of goods is considerable in volume. The US Customs and Border Protection (CBP),19 handled 20 million containers which arrived in the USA by ship, railway and road in 2005.20 This means that many American companies are also dependent on imports for their production activities.

Planning the enhancement of security in the supply chain was initiated in the USA after the first attack against the World Trade Center in 1993 and the attack against an American destroyer, USS Cole, outside Yemen in 2000. During the months after the events of September 11, the American government and customs launched a number of different programmes which now constitute a relatively comprehensive system for imports to the USA. They consist of both legislation and voluntary cooperation between companies and authorities, primarily the American customs authority, CBP.21

Customs-Trade Partnership Against Terrorism (C-TPAT) is the core of the system – a voluntary certification programme that is intended to guarantee that importers are not subjected to more inspections than they were prior to September 11,

Advance Manifest Regulation (“24-hour rule”), legislation that requires that goods that are imported into the USA shall be notified to the American customs 24 hours before they leave the port of shipment,

Container Security Initiative (CSI), a network of security-certified ports outside the USA with American customs personnel stationed there,

Free and Secure Trade (FAST) is an agreement between the USA, Canada and Mexico which regulates the coordination of customs clearance between the countries and has the aim of speeding up the processing of certified companies and carriers at border crossings,

Automated Commercial Environment (ACE) which is the American customs authority’s initiative for electronic submission of information and customs clearance.

The various initiatives were not originally produced to form a system. In some cases there are links between them, although they can well be described separately. There is reason to consider whether the systems fail to cover certain areas and whether the systems overlap. If they overlap each other there is scope to re-use information, to change rules and to provide relief for companies. The reason why the initiatives are not more highly coordinated in the USA is partly a consequence of

---

19 In the text below, the US Customs and Border Protection is referred to either as the American customs or CBP. CBP is an authority under the Department of Homeland Security.
21 There is more information on the different programmes at www.cbp.gov
the political process – Congress grants funds for separate initiatives and has problems in linking the
different systems together in its administrative processes. However, it is the most comprehensive
system that any region has devised and constitutes a model and a point of reference for the work
being done to secure the transport chain in other regions. There can be reason to point out that C-
TPAT refers to imports only. It is only in the field of air transport that there are rules for exports.

Moreover, the USA has supported the production of the WCO’s SAFE Framework and is working
actively to establish regular cooperation with customs authorities in different countries and regions,
not least the EU. Therefore, it is important to obtain a good understanding of the way in which the
American system is constructed and what concrete importance it has for companies. The development
of security systems in the USA has proceeded relatively rapidly and there is a growing amount of
criticism from companies in the USA against the system and against its further development.22

4.1.1 C-TPAT

According to the American customs, the Customs-Trade Partnership Against Terrorism (C-
TPAT) is an initiative that has the aim that companies and authorities shall work together to
strengthen and improve the entire international supply chain. C-TPAT only applies to imports to
the USA. When the initiative was started in November 2001, with seven participating companies,
its focus was on attempting to create a system that would enhance the resistance of the supply
chain against terrorist attacks. The idea was that, if a terrorist attack took place, the largest
operators in terms of volume and value would be able to rapidly get their supply chains working
again and thereby reduce any harmful effects on industry. Initially few benefits with the system
were promised; the American customs could only guarantee that certified companies would not
be subjected to a higher frequency of inspections than before September 11. However, in the
American custom’s strategic plan for C-TPAT23 more ambitious goals are expressed: to enhance
security for a significant proportion of the consignments arriving in the USA; to give both benefits
and incentives to those companies that fulfil or exceed the requirements laid down in C-TPAT, and
to concentrate CPB’s resources on the consignments that are assessed to have the highest risk.

C-TPAT primarily includes companies with operations in the USA and certain specially invited
foreign manufacturers (see fact box 4.1). The objective of the selection of companies to participate
in the programme was to select those companies that are directly responsible for parts of the
transport chain into the USA and that constitute a low risk but handle a large volume.

| • US importer of record |
| • Highway carriers in USA/Canada |
| • Highway carriers in USA/Mexico |
| • Rail carriers |
| • Sea carriers |
| • Air carriers |
| • Marine port authorities/terminal operators in the USA |
| • Air freight consolidators/ocean transportation intermediaries and Non-Vessel Operating Common Carriers (NVOCC) |
| • Mexican and Canadian manufacturers/industries |
| • Certain specially invited foreign manufacturers/industries |
| • Customs brokers in the USA licensed by CBP |

Fact box 4.1 Types of companies included in C-TPAT

22 See, for example, U.S. Chamber of Commerce (2007).
23 US Customs and Border Protection, Securing the Global Supply Chain, Customs-Trade Partnership Against ter-
rorism (C-TPAT) Strategic Plan, (2004).
In February 2007 more than 10,000 companies had applied to participate in the programme and 6,375 had been accepted as certified partners. Of these 3,916 companies had been validated. A detailed description of the certification and validation process is provided below.

Which processes are included in the programme?

A company that intends to be C-TPAT certified must meet requirements in a number of different fields. The requirements are different for different types of companies and the role they have in the supply chain, but there is a considerable degree of overlapping between the requirements. There is extensive documentation for each category of companies on CBP’s website. For example there are categories for importers, customs brokers, rail carriers, foreign manufacturers, road carriers and sea carriers. Below, as an example, we have chosen to reproduce the requirements for importers since this is one of the more extensive fields and is of great relevance for companies that are not based in the USA.

Importers must conduct a comprehensive assessment of their entire international supply chains, defined from point of origin (manufacturer, supplier, vendor) to the point of distribution. The areas in which there are requirements on importers in C-TPAT are listed in summary form in fact box 4.2 below.

**Fact box 4.2 Requirements for importers in C-TPAT**

- Business partner requirements
- Container security
- Physical access controls
- Personnel security
- Procedural security
- Security training
- Physical security
- IT security

Business partner requirements

C-TPAT requires that the participating companies have very extensive cooperation with their partners in the supply chain. At the same time there are strict requirements that the importers shall have documented routines for the selection of business partners. Where those partner companies that are eligible for C-TPAT certification are concerned, the importer must have documentation that shows business partners’ potential status in C-TPAT. For those partner companies that are not eligible for C-TPAT certification, it is necessary to have written documentation to show that they can comply with the security requirements specified in C-TPAT. This can be verified by contracts, certificates/letters from managing directors or similar, by a certificate showing that the company complies with the WCO’s SAFE framework issued by a foreign customs authority, or by completing a questionnaire on the importer’s security status.

Great importance is attached to the place where a product is packed or consigned from. An importing company must ensure that its business partners have satisfactory routines that prevent the cargo being changed or manipulated in any way when it is dispatched. Both processes and premises must be regularly checked in respect of risks and they must fulfil the requirements stipulated by the importer.

Furthermore the importer shall ensure that their business partners document any connections with the security programmes of other customs authorities, that business partners have sufficiently sound finances that enable them to meet heightened security requirements, that they have the capacity to implement the measures, that they can identify shortcomings in security and then remedy the shortcomings.

---

Container security

It is important to prevent the introduction of unauthorised material or personnel into containers that are to be shipped. Therefore, in the packing stage, there must be routines for excluding non-authorised personnel and for sealing the cargo/container. Seals shall be used for all containers and they must meet or exceed the current ISO standard, PAS ISO 17712, for high security seals. Furthermore, the containers should be inspected before packing to ensure that they have not been damaged or modified and that locks work. There shall be written rules for ways in which seals shall be checked and affixed, including ways in which damaged seals or containers shall be recognised and how this shall be reported to the CBP or the foreign customs authorities concerned.

Physical access controls

The protection of premises and access to them when loading and storing containers must be satisfactory. Access to the premises shall only be given to authorised personnel. Access checks should exist at all points of entry and controls shall be made of employees, visitors, service providers, vendors, and so on. Employees should only have access to areas necessary for the performance of their duties. The company’s management or security department shall check, in a reliable way, the issue and recall of employee and visitor badges. Procedures for the issuance of keys, ID badges, codes etc must be documented. Visitors must present photo identification and have visitors’ badges that are fully visible. They must be escorted by the company’s personnel when on the premises. The same applies to suppliers and post messengers. All incoming consignments should be regularly checked from the security perspective. Routines shall be in place for dealing with unauthorised or unidentified persons.

Personnel security

The companies should have satisfactory routines for security checks on their employees and prospective employees. Where candidates for new positions are concerned, references and employment histories should be verified. In accordance with current legislation, it should be possible to make background checks of both prospective employees and employees, and periodic checks should made of employees who have sensitive positions or for whom there may be other reasons for checks. The companies must also have procedures for ways in which employees shall hand in keys, ID cards and codes to ensure that they are refused access to premises and systems when they are no longer employees.

Procedural security

Security measures must be in place to protect the processes that are relevant to the transportation, handling and storage of cargo in the supply chain. It is important here to ensure that all information used for customs clearance is legible, complete, correct, and protected against replacement, loss or changes. This includes protection of computer systems and access to information. Information concerning consignments from partners abroad must also be received in time and in the correct way. Information on the cargo/goods in the customs manifest must be correct and the description of the goods in respect of weight, marking and number of packages must be checked on arrival. Goods to be shipped must be checked in the same way against the order or delivery note. The identity of drivers who deliver or receive goods must be checked before the goods are handed over. All deviations from that stated in documents or agreed must be followed up and clarified. Customs and other authorities must be informed if illegal or suspected incidents occur.

Security training

A training programme should be established that makes the personnel aware of threats to the company. Special training shall be offered to personnel who are directly involved in dispatching or receiving goods or post. Special courses shall be offered on ways in which it is possible to ensure that goods to be dispatched shall not be tampered with by unauthorised persons, ways in which plans for internal conspiracies can be discovered, and ways in which access checks can be made secure. There shall be special incentives to achieve a high level of participation among the personnel for these courses.
Physical security
Stores and storage areas shall have physical barriers and deterrents that prevent unauthorised persons from gaining access. C-TPAT particularly emphasises fencing, entry and exit controls (manned or under camera surveillance), parking places that are separate from storage and loading, locking devices and key controls, adequate lighting in sensitive areas, alarm systems and video surveillance cameras.

IT security
C-TPAT requires that there is an IT policy in place that is followed up and is included in introductory training programmes or the like. All users shall have individual IT accounts that require a periodic change of password. The companies must have a system for detecting abuse of IT including improper access and altering business data. All system violations must be subject to appropriate disciplinary action for abuse.

COMPANY EXPERIENCE OF C-TPAT
H&M is a global fashion company with 1400 shops in 28 countries with more than 60,000 employees in the group. Germany is H&M’s largest market, followed by Great Britain and Sweden. In 2006, turnover including VAT amounted to SEK 80.1 billion and net profit amounted to SEK 10.8 billion. H&M does not own any factories. Instead it buys its products from some 700 independent suppliers and has some 20 production offices in different parts of the world, mainly in Europe and Asia. Shares in H&M are listed on the Stockholm stock exchange. Since 2000, H&M has had a presence in different parts of the USA and now has more than one hundred shops in the country. Sales in the USA amounted to approximately USD 664 million in 2006.

H&M has participated in the security programme C-TPAT since June 2004. When H&M chose to join C-TPAT it was primarily a strategic decision. The company made the assessment that it was necessary to be C-TPAT-certified in order to do any business at all in the USA. The objective was to facilitate the company’s operations in the USA by obtaining simplified trade and customs procedures. This was achieved by improving H&M’s overall standards for its work in the supply chain so that they complied with the conditions specified in C-TPAT. When becoming a member in June 2004, H&M was given Tier 1 status on C-TPAT’s three-tier scale. However, since 2006 H&M has been upgraded to Tier 2 status.

The advantages of membership in C-TPAT have largely been the improvements made to H&M’s standards in the supply chain which, in turn, have led to faster import procedures (for example noticeably fewer security checks of freight when importing). Moreover, H&M, through C-TPAT’s security initiative, has developed close cooperation and better communications with American authorities, for example the American customs.

Recently H&M presented an activity plan on ways it meets C-TPAT’s requirements in different security phases. It will be implemented in a way that takes into consideration the requirements contained in other security programmes (which have been accepted by American authorities). H&M is currently making a cost analysis of all its supply chain activities that have been changed as a result of security requirements.

H&M is also preparing an application for membership of the Canadian security programme PIP (Partners in Protection). In addition it is also preparing applications for membership in the EU’s AEO programme which started on January 1, 2008.

25 www.hm.se
Validation process

As a basis for certification, all companies that wish to be certified must make a self-assessment in accordance with the guidelines issued by the American customs. CBP then evaluates the information presented by the companies and decides on certification. Certification must then be validated. CBP requires the companies to develop their own validation processes that guarantee compliance with the content of their Supply Chain Security Profile and other documentation submitted to the CBP. Thereafter, Supply Chain Security Specialists from the American customs and the C-TPAT applicant jointly conduct a validation of the company’s supply chain security procedures. The aim of the validation is to check that the company has implemented the measures it has stated and to ensure that the key security measures are effective. In the validation process the status of the measures is evaluated in order to possibly give the company best practice status and thereby qualify for the third tier.

Validation shall not take more than ten days of the company’s time, even if the process in its entirety can extend over a longer period. After the validation procedure is finished, the American customs go through the information and confirm the validation. The companies that are selected for validation always receive a written request for this at least thirty days in advance together with a request for any supporting documentation needed. The selection of the companies is based on their risk level in respect of security-related problems in earlier checks, strategic threats in certain regions, other information about risk levels, and volume of imports.

Normally the company’s representative for the validation process is contacted in advance by telephone. On this occasion there is a discussion of the company’s role in the C-TPAT programme, the scope of the validation and the locations in the company’s international supply chain that shall be visited during validation. A validation visit normally does not take more than one day. During this visit the company’s security procedures are examined in detail. The company receives a written report on the findings of the validation visit. The report gives recommendations and identifies best practices where appropriate. If significant weaknesses are revealed, the company can have its C-TPAT benefits suspended and it will no longer be able to enjoy the advantages in respect of customs treatment linked to this. In such cases C-TPAT recommends the company to produce an action plan to address the weaknesses.

What benefits does C-TPAT give the companies?

The benefits of participating in C-TPAT vary depending on the security level the company has achieved. Since May 2005 the American customs has used a three-tier scale for the ways in which they treat the certified companies. In the first tier certified companies receive from the CBP a lower risk factor assessment which results in fewer inspections for security reasons, fewer inspections concerning general compliance with the rules, and exceptions from most of the selection criteria for checking goods from the trade perspective. These measures in combination are intended to give the companies a low level of inspections. In addition to this, companies are given a certain degree of priority if examinations must be made and can be granted a certain degree of mitigation in respect of penalties for violations of American customs legislation. In practice it would appear as if companies benefit from most of these advantages in the second tier and that differences from not participating in the first tier, where no validation is currently performed, are small. On the other hand, the first tier is a prerequisite for gaining access to FAST and the Importer Self Assessment programmes (see below). However, in this connection it should be emphasised that checks of foodstuffs, veterinary checks etc are not affected by these rules.

Companies that have their partnership validated join the second tier. The companies that can show that they have fulfilled the lowest level of security criteria specified for different types of companies (sea carriers, road carriers, railway carriers, foreign manufacturers, importers and others) qualify for the second tier. The companies receive the same advantages as in the first tier but twice the level of risk reduction given by the American customs. This results in significantly fewer inspections for security reasons.
To qualify for the third tier the companies must go further and adopt so-called best practices in respect of security. CBP issues a catalogue of best practices\(^{27}\). However, it states that qualification for the third tier is not necessarily dependent on implementing all the measures in the catalogue. It is a question of an assessment that is made from case to case during validation. In the third tier the risk factor assessment is lowered further with consequent very infrequent inspections for security reasons. The third tier is seen as a precursor for qualification for a future “green lane” procedure which will give the companies free passage through customs apart from occasional random checks, provided the goods have been shipped from a CSI certified port (see below) and that the containers have security seals affixed to them.

**Links to other initiatives**

C-TPAT can be regarded as the backbone of the CBP’s security system. It has specific links to other parts of the system. For example, certification in C-TPAT is a prerequisite for a company to be certified in the FAST programme and/or in the Importer Self Assessment (ISA) programme (see below). In addition, certain phases in C-TPAT require that CSI ports or ISO certified high security seals are used.

Another type of link is that which shows the effect on other regions’ security initiatives. BASC, a security programme which is a company initiative mainly involving South American companies, is described below. It has considerable points of contact with C-TPAT and most of the processes that are verified in C-TPAT are also to be found in BASC. BASC is the older programme but has also been developed with support provided by the American customs authorities.

It is an explicit ambition of the American authorities to spread information about their initiatives to other countries and the USA has been a driving force in the negotiations on the WCO’s SAFE Framework. For further information see chapter 3 on the WCO.

The EU and USA are also negotiating to see if it is possible to achieve an application of the American system and of the EU’s rules concerning Authorised Economic Operators (AEO), as well as the advance notification of imports and exports, which harmonises all three components as much as possible. Read more about the negotiations in the section on the EU.

**A case study gives a description of the present situation**

In a case study made in 2006, three researchers from Kansas University\(^{28}\) established that there are considerable similarities between C-TPAT and the ISO system (see this section) in respect of quality standardisation since both systems focus on descriptions of general, rather than actual, generic security or quality. Even the certification processes themselves have great similarities. It can therefore be assumed that certification in C-TPAT, as well as ISO certification in respect of quality, constitute a good point of departure for further work on security. This is also confirmed by companies that have been partners in C-TPAT for a number of years; more requirements are made of them and their work on security has required more resources over time. At the same time companies can show less shrinkage and fewer thefts, as well as a better organised supply chain. It would appear to be the case that even if participation in C-TPAT involves costs, there is also an income side apart from the expected benefits of fewer examinations and faster customs clearance.

The Kansas study shows interesting results despite the fact that it is only a small case study of five companies. It points out success factors in the companies that have implemented the certification process and the results of the certification. The study shows that it is necessary that top management supports the project, that the certification team represents different functions in the company, and that training is a necessary instrument for success with certification. At the same time major IT changes do not appear to be necessary for certification – none of the studied companies were obliged to implement any major IT updates to obtain better control over their flow of products.

---


\(^{28}\) Sheu et al. (2006), 263-274.
Furthermore, the study shows that the benefits certification was assumed to lead to were actually achieved. The four companies that had been C-TPAT partners for a sufficient period of time to experience benefits confirmed that they had faster border inspections, lower costs and greater customer satisfaction. In addition, the study appears to confirm that the CBP’s explicit goal of promoting international cooperation between the companies in order to create a more secure supply chain has been achieved. On the other hand, the research team from Kansas University considers that it is uncertain whether enhanced security has actually been achieved through cooperation. They refer to the similarities with the ISO programme and the doubts that the companies express in respect of this. The researchers are of the opinion that C-TPAT should be seen more as a means of making security work more effectively than as an ultimate goal which, in itself, means greater security.

C-TPAT evaluated on behalf of the American customs

In an evaluation of costs and benefits made by the Center for Survey Research at the University of Virginia for the CBP, published in August 2007, it is shown that the programme provides benefits in terms of reductions in the number of inspections, fewer thefts and less shrinkage. Responses to the study, which had a response frequency of 29.3 per cent, were made by 1 756 companies and organisations, of which 62 per cent are based in the USA. 54 per cent of the respondents were importers. Regardless of the sector in which the companies are active, they state that the possibility of saving time and costs when passing through customs was the main reason for participating in the programme. For the importers the most important reason was to avoid disruptions in the supply chain. Almost one-third (32.6 per cent) of those who responded stated that the benefits of the programme outweighed the costs, while a quarter (24.2 per cent) stated that the costs and benefits were approximately of the same value. Some 16.8 per cent stated that the costs outweighed the benefits and 26.4 per cent stated that they felt it was too early to make an evaluation.

One-third of the companies that responded (35.4 per cent) stated that they had had fewer inspections by the CBP. Slightly more than half of these stated that the number of inspections had decreased by more than 50 per cent; 6.6 per cent stated that the number of inspections had increased, while 44.1 per cent stated that the number of inspections was unchanged.

Furthermore, the study confirms that there are benefits inasmuch as the companies obtain better order in its logistics and a reduction in shrinkage and thefts, even if these benefits are felt to be unevenly distributed among the companies.

Where does the supply chain end?

One question that arises through the security initiatives introduced by the customs authorities in different countries is the point where the supply chain actually starts. In the C-TPAT programme, participating importers must ensure that their suppliers work in accordance with corresponding security standards and are certified in corresponding programmes, if such exist, in the country in question. The requirements are far-reaching and there is reason to analyse how far back in the supply chain authorities require, or will require, importers to have controls. Since many importers have never visited their foreign suppliers, the idea of a partnership that runs throughout the entire supply chain can be overwhelming. A study made by the First Advance Corporation points out weaknesses in controls of suppliers in C-TPAT. According to this study, less than 10 per cent of business partners are checked. In C-TPAT it is stipulated that business partners must be C-TPAT compatible but examinations and risk evaluations are not made. It is particularly difficult for companies to have resources to do this when the rules of C-TPAT are updated.

---

29 Diop et al. (2007).
30 Purtell (2007).
4.1.2 Container Security Initiative (CSI)

The Container Security Initiative was published in January 2002. It focused on a few ports that shipped the greatest volume of goods shipped to the USA. The background was once again the terrorist attacks of September 11, in combination with the fact that 90-95 per cent of the world’s trade is transported by sea in containers. A firm of consultants, Booz, Allen and Hamilton, stated in a report in October 2002 that it would cost USD 58 billion to close one of the major American ports for a period of twelve days to search for an explosive device. The system was further reinforced in 2006 by the so-called SAFE Port Act (see below).

In brief, the point of departure of CSI is that ports with a sufficiently high technical level of security and control equipment are certified and have customs personnel from the USA stationed there. This means, in principle, that the USA thus moves its border to the port in question. Goods that arrive in the USA from CSI ports can thus be cleared very rapidly. All that needs to be done is to check that the seals and containers are unbroken and that all documentation is in order. The rule relating to 24-hour advance notice of goods that are to be shipped to the USA further supports the system. If this corresponds to practice in the American ports is, however, not borne out. Information on the freight on the advance notification is processed again since some time passes while the ship is at sea. The way in which the cargo is then handled can be determined by local routines.

The main parts of the initiative

The main objective of the CSI is the early identification and inspection of containers that can be used for terrorism. The American customs use an automated system to make a selection, which reflects the large number of containers that pass American borders. For this purpose, containers are checked in advance and investigated electronically or manually as early as possible in the supply chain, often at the port of shipment. As far as possible, technical equipment is used to examine the containers. X-ray and gamma ray technology must be available in CSI ports, as well as radiation detection technology. This is the basis of the so-called Non-Intrusive Inspection (NII), i.e. inspections are made without having to enter a container physically, which is often costly and can create delays in the flow. In addition, the development of smart containers is part of the strategy. With the aid of Radio Frequency Identification (RFID) technology and smart security seals it is possible to identify the containers that have been manipulated since loading. The seals prescribed in C-TPAT are, however, still mechanical, even if they are of the highest security class.

The system also offers possibilities for other countries to have corresponding requirements in respect of the USA. At present Japan and Canada have personnel stationed in American ports.

The scope of the system

Today, about 90 per cent of all transatlantic trade and the trade in goods over the Pacific Ocean to the USA are inspected in advance. The CSI will continue to expand in places that are assessed to be of strategic importance around the world. Furthermore, in the future the CBP intends to stipulate that an ISPS code (see above in chapter 3) shall be required of all ships that call at ports in the USA.

At the end of November 2007, 58 ports around the world were certified CSI ports: 23 in Europe, 20 in Asia, two in Africa and 13 in North and South America. The complete list can be found in appendix 1. The fact that there are only two ports in Africa raises the questions of whether there is a risk that the system will make it more difficult for developing countries to participate in international trade. Likewise, the focus on major ports is also a source of concern. However, the CBP maintains that, with the resolution adopted by the WCO in 2002, all ports in its member states can develop programmes similar to the CSI programme. In 2004, the EU and the USA agreed to study whether it was possible to extend the number of ports in Europe that can be feeder ports to the CSI ports. The idea is that these ports shall have the same equipment but be manned by national customs authorities.

Requirements in respect of CSI ports

The countries that want their ports to be CSI ports must fulfil a large number of requirements. Their customs administration must be technically capable of implementing NII inspections of all goods that are imported, exported, in transit, or transhipped through the country in other ways. The port in question must have direct, regular and substantial container traffic to ports in the USA. The port authorities, together with the customs, must undertake to produce a risk management programme that can identify possible high risk containers. Furthermore, the country’s authorities must be prepared to share information with the USA and CBP to facilitate a joint focus on high risk objects, and be prepared to introduce an automated mechanism for this exchange of information. This can be a problem for many countries. An agreement reached in 1988 between the USA and Sweden, for example, only allows the Swedish Customs to share information from case to case. Furthermore, the port must make a review of its infrastructure to identify vulnerable parts of the port facility and processes and must be committed to resolve any problems. Moreover, the port must have a programme to protect its personnel similar to that described in C-TPAT.

Advantages and problems

The CSI system clearly has many advantages for the participating ports, the host countries and companies that use the ports, and for the general maintenance of security. The participating ports are automatically given a competitive advantage over other ports and can also benefit from certain technology and transfer of know-how supplied by the USA. For the host countries it can be a strategic issue of considerable importance – according to the Swedish Customs an argument of this type lies behind the participation of the port of Gothenburg in CSI. In-depth cooperation between customs authorities in different countries should lead to greater trust, better coordination and a simpler system. This, in the final analysis, benefits the companies. For this reason the CSI is also supported by the WCO and EU and a number of other organisations. CBP mentions trade facilitation as a driving force behind the CSI. Where companies are concerned, there are benefits in terms of time and security. The security inspections of goods in the shipping port and the smooth passage they are given when they are unloaded in the USA saves time since the handling of goods in the shipping port most often leads to waiting time – waiting time that is now utilised. Better security and better controls are in the interests of the companies since it leads at the same time to fewer thefts and less shrinkage.

Many countries still do not have a CSI port. It is the American authorities that make decisions on the ports that shall be given CSI status and these decisions can be assumed to have an effect on trade flows. Most modern ports already have a high level of technical expertise and advanced equipment but it cannot be excluded that the CSI contributes to distorting trade and affecting transport routes. The fact that there are only two CSI ports in Africa could be a problem, for example from the perspective of sustainable development, even if there is only a small amount of container traffic from Africa today, due to its road network. In this connection the requirements stipulated in C-TPAT also have an effect depending on how far back in the supply chain one wants to take security initiatives.

4.1.3 Advance Manifest Regulation (“24-hour rule”)

The rule concerning the advance notification of goods that shall be shipped by container to the USA 24 hours before the goods are loaded on a ship was introduced in January 200.4 The rule makes it possible for customs personnel in the USA to make an advance examination of high risk consignments before a container is loaded in a foreign port. If a company breaks the rule the result may be legal action and permission to discharge the entire ship may not be given. The Customs’ Automated Targeting System (ATS) applies hundreds of pre-programmed selection criteria to determine the

---

33 Ordinance (1988:146) on the implementation of an agreement between Sweden and the United States of America on mutual assistance in customs matters.
34 U.S. Federal Register, Department of the Treasury, Customs Service: “Presentation of Vessel Cargo Declaration to Customs Before Cargo is laden Aboard Vessel at Foreign Port for Transport to the United States”, Oct. 2002.
containers that shall be extracted for inspection and each consignment is given a factor based on terrorist risk. It is assumed that the ports included in the CSI programme work on sharing information and efforts are being made to avoid ATS providing reports on false problems or erroneous suggestions for controls. ATS will constitute a part of CBP’s electronic customs environment: the Automated Commercial Environment (ACE) and CBP hopes that when this has been fully introduced it shall be possible to process and link together larger amounts of information that is collected even earlier.

The information that shall be provided on the advance manifest is:

- Foreign port of departure
- Carrier’s Standard Carrier Alpha Code (SCAC)
- Voyage number
- Date of scheduled arrival
- Numbers and quantities from the carrier’s bills of lading
- The first port of receipt of the goods
- Precise description of the goods and/or the Harmonized Tariff Schedule (HTS) code
- Shipper’s complete name and address or identity number
- The consignee’s name and address or identification number
- Vessel name, national flag, and vessel number
- Foreign port where the cargo was laden on board
- Hazardous material indicator, if cargo of this type is to be shipped
- Container number
- Seal number affixed to the container

The rules are not intended to affect the total time the vessel must stay in the port. Here it would be interesting to see the effects the rules have had in practice. Prior to the introduction of the advance manifest rules, time spent in ports was normally some 24 hours and loading and unloading activities were started directly. The fact that the advance notification must be made 24 hours before a container is loaded means, in other words, that when the vessel has arrived in the port there is no time for advance notification of new shipments. Last minute shipments cannot be taken on board. For the consignors this leads to a situation in which their capital is tied up and they have less flexibility. At the same time it has the effect that it is easier for the shipping companies to plan the cargo.

Where air transport is concerned, the information shall be submitted to CBP directly after the departure of the flight. This makes it possible for the CBP to identify high risk goods through their Automated Targeting System (ATS).

CBP has promised to review the rules when the Automated Commercial Environment is in full operation, but no review of this type has yet been made.

### 4.1.4 SAFE Port Act

In October 2006 the American Congress approved further consolidation of the legislation in respect of port security in the so-called SAFE Port Act. This is an extensive legislative package which includes, among other things, strengthening CSI and C-TPAT. In addition, the package contains instructions to the Department of Homeland Security to produce a proposal on ways in which further information can be submitted in respect of cargo and transport to American

---

35 A C-TPAT certified company can be given a code that states the company’s identity: Standard Carrier Alpha Code.
36 The HTS code is an eight-digit combination of figures that specifies the goods contained in the consignment. HTS is an extension of the international HS code and is linked to the CBP’s customs tariff system.
37 The International Maritime Organization is a UN agency that was established in 1948. The IMO number is a seven-digit number that gives each ship a unique registration number. [http://www.imo.org/TCD/mainframe.asp?topic_id=388](http://www.imo.org/TCD/mainframe.asp?topic_id=388)
ports with the aim of making a better risk assessment. The proposal is referred to informally as “10+2” – usually with a reference to the SAFE Port Act. In addition to the information which is already included under the “24-hour rule”, in its proposal for implementation CBP has identified the following ten items of information which it proposes shall be given. According to CBP, the information has been selected since it is relatively easy to obtain from existing logistical processes:

- Manufacturer’s name and address
- Vendor’s name and address
- Container loading location
- Consolidator’s name and address
- Buyer’s name and address
- Ship to name and address
- Importer’s number (if registered at CBP)
- Consignee number
- Country of origin of the goods
- Commodity classification code

In addition to this, the CBP will require shipping companies to provide two more sets of data: the vessel’s stow plan and container status messages. The importer and carrier are the parties that will primarily be obliged to provide the information and they will be able to do it through the computer systems which they normally use to communicate with CBP and, at a later stage, in the Automated Commercial Environment (ACE).

It is difficult to reconcile SAFE Port Act’s “10+2” with the limitations on the amount of information which can be requested from companies according to the WCO’s SAFE framework. The proposal has not yet been adopted but will probably enter into force in 2008. However, the USA has informally presented a “10+2 initiative” to the WCO with the hope that, at its annual council meeting (which takes place in June each year) the WCO will review its advance notification rules and possibly include more information to make them correspond to a greater degree with “10+2”. The question is whether the USA will allow the “10+2 initiative” to enter into effect before the WCO possibly revises its rules or whether it will await this revision.

4.1.5 FAST

The Free and Secure Trade (FAST) programme is a so-called border accord initiative between the USA, Canada and Mexico. The participating countries have agreed to coordinate, to the maximum possible, their processes for the clearance of shipments at the border. The companies that can participate in FAST are carriers, drivers, importers and manufacturers (the last mentioned only at the southern border of the USA). They must submit an application, agreement and security profile, depending on their participation in the C-TPAT or FAST programmes. The basic concept is that known companies shall be given rapid treatment at the borders so that the American customs can concentrate on high risk goods. Even during times of heightened alert levels it should be possible to regard FAST goods as low risk transports that can be handled in the same way as usual.

CBP emphasises several benefits for companies and individual drivers to participate in the programme. At a number of border crossings there are special FAST passages (dedicated lanes) with faster clearance. The companies can count on having a lower number of inspections as they show that they are complying with the requirements in FAST. Moreover, they will have a close partnership with the administrations of C-TPAT and PIP (the Canadian customs authorities’ certification programme, Partnership in Protection). The programmes should lead to a higher

---

39 In November 2007 the SAFE Port Act’s “10+2” is in a so-called “Proposed Rule Making” process, i.e. the proposal is being circulated for comment to the federal authorities in the USA.
degree of security in the supply chain and fewer disruptions. In addition, the carriers have the security of knowing that their partners also participate in C-TPAT as importers or, where Mexico is concerned, as C-TPAT manufacturers.

One special feature of the programme is that individual drivers can also obtain a special FAST commercial driver card, which makes them an important part of the system. In order to use FAST passages, trucks must be a C-TPAT carrier, carrying transport goods from a C-TPAT approved importer, and the driver must be in possession of a FAST commercial driver card. At the southern border the manufacturer must also be an approved C-TPAT participant and containers must have seals that correspond to CBP’s requirements in respect of high security seals. In other words, the requirements are higher for the transports between the USA and Mexico than those between the USA and Canada.

There are two methods for the customs clearance of goods in FAST. One is also called FAST and is a paperless system which, with the aid of electronic data transmission via transponders, makes it possible for customs to process goods at the border more or less without the vehicle having to stop. The other method is called the Pre-Arrival Processing System (PAPS). This is an automated method for processing goods with the aid of bar codes. This makes rapid customs clearance possible at the same time as each shipment is processed in the Border Cargo Selectivity (BCS) system and the Automated Targeting System (ATS). ATS is a system for assessing risk levels and was briefly described above in the section on the 24-hour rule. BCS is an automated system for determining risk levels and the need of inspections.

4.1.6 Importer Self-Assessment (ISA)

The Importer Self-Assessment programme is a partnership programme for those companies that fulfil CBP’s trade and customs rules. Companies that can show that they have two years’ experience of importing in which they have closely followed CBP’s rules and information collection processes can apply to participate in the programme. Membership means fewer inspections, faster customs clearance and a higher degree of automated transfer of information. CBP maintains that it is a programme in which the focus lies on trade facilitation, in other words it is not a security programme in the real sense of the term. However, membership is only granted to companies that give priority to security in the supply chain – in practice those that are already participating in C-TPAT. CBP also states that it is an advantage to participate in both programmes since security and customs processing are often the responsibility of different departments in a company. CBP states that the procedure from application to approved membership normally takes four months.

4.1.7 Secure Freight Initiative

In December 2006, The American government’s Department of Homeland Security and Department of Energy launched an initiative that has the aim of strengthening the ability of the American authorities to trace nuclear and other radioactive substances at borders. The initiative, which is called the Secure Freight Initiative (SFI), is financed by the two departments in an amount of USD 30 million each. Since the beginning of 2007 the latest technological equipment has been placed in seven foreign test ports: Port Qasim in Pakistan, Puerto Cortés in Honduras, Southampton in the United Kingdom, Salalah in Oman, Singapore, Busan in South Korea and Hong Kong in China. The idea is that it shall be possible to stop and secure containers containing radioactive material and which can otherwise constitute a threat to the global supply chain in maritime transport at the port of shipment.40

4.1.8 Operation Safe Commerce – support for research

Operation Safe Commerce (OSC) is an initiative that was started in July 2006 to provide support to research projects initiated by companies to improve security in the international supply chain. It is basically system financed by Congress for companies’ research programmes.

40 [www.cbp.gov/cgov/newsroom/fact_sheets/sfi/](http://www.cbp.gov/cgov/newsroom/fact_sheets/sfi/)
4.1.9 New legislation on 100 per cent scanning of containers

On August 3, 2007, the “Implementing Recommendations of the 9/11 Commission Act of 2007” was signed into law by the President of the United States. The act includes a large number of measures to improve security both inside and outside the USA. A large part takes up measures for overland transport and intermodal\textsuperscript{41} transport. Of greater importance for international trade are the rules introduced on 100 per cent scanning of containers for both air and maritime transportation.

Section 1602 of the act lays down that no later than three years after the law enters into force, i.e. in 2010, all cargo that is transported on passenger flights into or from the USA shall be screened.\textsuperscript{42} This means that goods will be handled at least as securely as baggage, i.e. if baggage is X-rayed, cargo must also be X-rayed. Today the American regulations for air freight are similar to the European regulations (see below in this section).

Furthermore, section 1701 lays down that the Department of Homeland Security shall draw up a plan for ways in which it shall be possible to scan 100 per cent of all goods containers in foreign ports on route to the USA in order to detect radioactive material. The scanning shall include both radioactive scanning and scanning with gamma ray technology to detect unknown objects. The plan shall be implemented by 2012 at the latest and contain annual indicators on the degree of progress that has been made towards the goal. However, the Secretary for Homeland Security can report to the US Congress if it is not practical or technically possible to achieve the goals, if this proves to be the case.

The legislation has encountered extensive criticism in the USA\textsuperscript{43} and other countries. American chambers of commerce, among others, have drawn attention to the negative effects on trade. The European Commission has expressed its points of view in, among other things, a press release from László Kovács, the Commissioner for Taxation and Customs Union\textsuperscript{44}. Kovács is of the opinion that better risk analyses and improvements in the selection of containers for scanning purposes should provide a better balance between security aspirations and trade facilitation. He also regretted the fact that the US Congress has not awaited the results of the pilot projects being run jointly by the American and European customs authorities.

4.2 Canada

Canada has not developed a system of complementary security programmes to the same extent as the USA. To a large extent Canada is undergoing a process of further development, partly in respect of its programmes of cooperation with the USA in FAST and C-TPAT, and partly its own initiatives that have mostly focused on preventing contraband smuggling and illegal immigration. The Canadian customs, Canada Border Service Protection – Agence des services frontaliers du Canada (CBSA-ASFC), works more on a regional basis than its counterpart in the USA, CBP. Canada has also participated in the Container Security Initiative (CSI) since October 2005 and CBSA has its own personnel in ports in the USA. See also the section on CSI under the USA.

4.2.1 Partnership in Protection (PIP)

The Partnership in Protection (PIP) initiative was started in 1994 under the name Carrier Memorandum of Understanding Program (MOU). It was reinforced after 2001 as a consequence of the acts of terrorism in the USA. It is a voluntary programme which initially focused on preventing contraband smuggling and enhancing compliance with the rules by participating

\textsuperscript{41} Transport by more than one mode of transport.
\textsuperscript{42} Screening is a term for methods to identify goods for inspections. Scanning is control by means of X-ray, gamma-rays or radioactivity measurement.
\textsuperscript{43} \textit{USAtoday} (2007); SecurityInfoWatch.com (2007). See also letters from the American Association of Exporters and Importers, and the Business Alliance for Customs Modernization, among others, to Senators Liebermann and Collins.
\textsuperscript{44} European Commission (2007).
companies. Canadian legislation stated that modes of transport used for smuggling could be seized by the authorities. This had the effect that companies jointly contacted the Canadian authorities to find a way of showing that they had done everything to prevent smuggling. The programme now focuses more specifically on preventing crime and terrorism and on strengthening security in cross-border trade. CBSA has stated that it wants to upgrade the programme to make it fully compatible with the WCO’s SAFE Framework\(^{45}\) (see this section) and with the American customs’ certification programme for security, C-TPAT. Membership in PIP is necessary for Canadian companies to participate in the Free and Secure Trade programme (FAST). (See section on the USA.)

PIP is principally based on enhanced security, exchange of information, and awareness sessions on security risks. Companies wishing to participate in the programme sign a partnership agreement with CBSA. In itself the agreement merely states that the company will cooperate with the customs to create secure trade. Once the agreement has been signed, the regional PIP representative in each province contacts the company to see how PIP can be implemented. A security questionnaire and a company information sheet must be completed within 60 days after the agreement with CBSA has been signed. The security questionnaire is a self-assessment based on guidelines issued by the CBSA.

According to the CBSA, where the companies are concerned, PIP provides the following benefits: faster processing of shipments and passengers, improved security, greater familiarity with customs requirements among the company’s personnel, advisory services from CBSA which examine the company’s security procedures, and an enhanced reputation for the company. Compared to C-TPAT, CBSA provides very few details on the specific measures that must be taken for the company to participate in PIP. In the information it provides, CBSA focuses much more on security in general and measures to counteract smuggling and theft than on measures to counteract terrorism. Nor does PIP provide benefits in stages for companies in their contacts with the customs authorities. The work and benefits from the work are more at the individual company level.

In October 2006, 1 320 companies were members of PIP and the great majority of them were carriers (1 045). Importers also constituted a large group – 218. An evaluation made by CBSA in October 2006 showed that this, as expected, is a relatively small proportion of all importers – estimated at some 17 000. Some 80 per cent of the companies that participate in the programme are Canadian. The report points out that one reason for the low level of participation is a lack of resources. The lack of local CBSA representatives and continuity in their training and employment has been a bottleneck in the system and an internal evaluation has shown that many companies have not been given access to all parts of the programme that concern them, for example on site security reviews or security recommendations.\(^{46}\)

Moreover, the level of manning in the programme is lower compared to its American counterpart. According to the report, CBSA officers who handle PIP partners have 56.3 partners per officer while the corresponding figure for CBP officers working with C-TPAT companies is 37.3. The fact that the programme’s only concrete benefit for companies is that it is a prerequisite for participation in FAST can possibly explain why carriers are overrepresented among the participants.

Furthermore, the report points out that companies report results arising from their participation which were not expected at the outset. These include fewer thefts, fewer problems with goods that have been tampered with or destroyed, and better health and safety for employees. These are results that have also been mentioned in studies of C-TPAT companies.

---

\(^{45}\) World Customs Organization (2005).

\(^{46}\) Canada Border Services Agency (2006).
CBSA’s internal report proposes a large number of improvements. From the international perspective the most significant are the proposals to harmonise PIP even more with C-TPAT and that participation in PIP shall be the basis for companies wishing to become AEO (Authorised Economic Operators), in accordance with the WCO’s definition of the concept. (See section on WCO.)

4.2.2 Advance Commercial Information

In April 2004, CBSA started an initiative to improve security in container traffic to Canada. The programme was entitled Advance Commercial Information (ACI). It is a system for advance notification of goods which to a great extent resembles both the American legislation on 24 hours’ advance notice and its European counterpart (see these sections). Container goods that shall be sent to Canada must be notified to the Canadian Customs 24 hours prior to loading in foreign ports. In a second phase which started on December 12, 2005, air freight was also included. The air carriers or freight forwarders must transmit air cargo data electronically to CBSA four hours prior to loading at a foreign airport or, if the flight time is less than four hours, at the time of departure.
5 Security initiatives in South America

5.1 Business Alliance for Secure Commerce (BASC)

The Business Alliance for Secure Commerce (BASC) is a voluntary security initiative that was initiated by a North American company that imported goods from Latin America via the port in San Diego, California. BASC refers in the first place to trade with Latin America and the vast majority of its participants are Latin American companies. A proposal was presented to the American customs on the introduction of security measures in the supply chain that would reduce the risk of legitimate cargo being used by illegal organisations for smuggling drugs, theft, and the dissemination of different types of contaminated cargo. When the programme was introduced, the emphasis was placed on combating smuggling, and during the first few years the programme had the name “Business Anti-Smuggling Coalition”. Since its introduction in 1996, BASC has developed into an organisation that secures the integrity of the supply chain and covers a large number of security issues in the chain. Currently it is one of the programmes that have the most detailed lists of security standards (some 100 security measures). At the same time the costs arising from not being certified can be very high. Some 40 per cent of the companies that were included in a case study of BASC (see below) stated that the principal reason for joining the organisation was that this was requested by customers or suppliers, that it was a requirement in order to export to other countries, or that certification functions as a form of market differentiation.

The World BASC Organization (WBO), BASC’s international umbrella organisation with its head office in Delaware, consists of representatives of national and regional BASC chapters, and BASC’s members are to be found in the private and public sectors, as well as among international organisations and associations. The private sector is represented by companies in the international supply chain which are active in logistics and other activities in international trade. The public sector is represented by customs authorities and international police organisations. In Europe, France, for example, is a member of BASC since its customs authority has joined the programme. The World Customs Organisation (WCO) and the USA’s Chamber of Commerce are two examples of organisations and associations that participate in BASC.

Certified companies can be informed about programmes and agreements organised by BASC, for example training of personnel in fields relating to security and international trade, participation in annual BASC seminars, certification reports and follow-up, cooperation agreements with local authorities, support for creating contacts with port authorities and customs administrations, and exchanges of information with other BASC chapters. Companies in countries that are not members of BASC can also be certified in the programme, but there are special rules for these companies.

5.1.1 Selection criteria

The World BASC Organization stipulates a number of requirements for companies that wish to become members of BASC:

- Only companies actively involved in logistics, production or service activities related to foreign trade can become members.

---

48 Ibid.
49 BASC chapters are to be found in Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Mexico, Peru, Pacific Ocean region and Uruguay.
50 A complete list of all BASC-certified companies is available at [www.wbasco.org](http://www.wbasco.org).
51 At the present time the following customs authorities participate in BASC: USA, Mexico, France, Italy, Colombia, Venezuela, Ecuador, Uruguay, Argentina, Dominican Republic, Nicaragua, Costa Rica, El Salvador, Panama, Bolivia (anti-drugs authorities and port authorities).
52 For a complete list of international organisations and associations that participate in BASC, see [www.wbasco.org](http://www.wbasco.org).
• Each company must be legally established and have commercial activities in the country, as well as overseas, that will permit the validation of the company and its partners and directors. Moreover, the company shall not have a criminal record or be suspected of crime either by national or foreign authorities.

• Each company must comply with the registration process that has been approved by the chapter concerned in accordance with the WBO’s procedures.

5.1.2 Application procedure

The process is initiated by the company sending an application to the BASC chapter (if there is no BASC chapter in the country in question, the application is sent directly to the WBO). The application shall be accompanied by documents that verify the company’s country of origin and legal status. A commission studies these documents and decides whether the company qualifies for the certification process. If it does, the company will be the subject of a security audit and will receive recommendations for changes in any fields where the company has shortcomings. Depending on whether the company fulfils BASC’s minimum requirements in respect of security it will either be certified or asked to make changes in areas where the company does not meet standards before a certain deadline. On certification a company undertakes to follow BASC’s guidelines. Certification is valid for one year and thereafter the company is evaluated annually to confirm that it is following these guidelines. The evaluation of member companies shall be performed by an auditor certified by BASC. Each company is responsible for ensuring that an evaluation is sent to the WBO each year but if problems arise and a new supplementary evaluation is required, this is also done by the WBO. In both cases the company bears the costs of the evaluation.

5.1.3 Security

BASC’s standards take up both practical and administrative aspects of security in the supply chain. An overview of BASC’s standards is given in fact box 5.1. Each company shall draw up a security strategy with associated security routines in the company. Before the routines are drawn up, the company’s organisation shall be analysed on the basis of whether or not it is able to comply with BASC’s requirements and the types of security risks that can arise in the future. The routines that are then drawn up cover a large number of issues, both administrative such as the handling of documents and files and checks of the background of personnel, and purely practical routines, such as checks of lighting and perimeter fencing. Thereafter the security strategy shall be updated at least once a year and the training of personnel shall take place successively.

In its security policy the company lays down how it shall relate to its personnel and to the authorities. Security standards shall be clearly defined and procedures for recruitment and reports on irregularities and suspicious activities shall be laid down. The security policies that are drawn up shall then be communicated to employees and customers through posters and the like at the workplace.

In general it can be said that BASC’s security measures are strongly reminiscent of the measures in C-TPAT (see section on the USA). Personnel matters, physical security, electronic security systems and procedures in respect of seals are all central features of both programmes.

As in C-TPAT great importance is attached to physical security. One central feature here is external security, i.e. fencing, doors and procedures for entry and exit to premises. BASC’s standards for physical security describe in detail how the company shall handle practical aspects of security such as checks of premises, keys and locks, training in security for personnel, ID systems, and routines for the receipt and delivery of goods. The security procedures for the reception of containers and inspection of vehicles that are not owned by the company are particularly detailed.

53 Recertification of companies in countries that are not members of WBO is administered by WBO. For more information see http://www.wbasco.org/english/documentos/certification_procedure_for_organizations_on_non_basc_countries.pdf
BASC companies shall have specific policies for the handling of cargo documents and signatures, as well as for deadlines for the reception and completion of documents. According to BASC, experience shows that last minute reception of documents is a tactic used by criminal organisations to avoid risk analysis of suspicious transports.

Another issue that is given considerable attention and taken up in detail refers to the routines concerning personnel security. Employees shall not only be checked on employment and when they leave the company. Checks of personnel and their social circle and their behaviour shall be made regularly.

Since BASC, as C-TPAT (see section on C-TPAT) have been developed in cooperation with the USA's customs authorities, it is not so surprising that there are many points of contact between the programmes. BASC is the older programme, and when C-TPAT’s security standards were introduced, BASC was one of the models. Both programmes emphasise the importance of physical security, personnel security, training of personnel and information handling. Since C-TPAT has hitherto been a programme for companies in the USA, much of its focus lies on relations with partner companies in other countries. This dimension, which in BASC’s standards is called security strategic alliances, is given less attention in C-TPAT. The reason can be assumed to be that BASC principally applies to companies that export to the USA, which means that they are one step further away in the supply chain than the majority of C-TPAT certified companies.

---

Fact box 5.1 BASC's standards. Source: [www.wbasco.org](http://www.wbasco.org)
COMPANY EXPERIENCE OF BASC

VIMARCO LTDA is a Colombian private security company that, with its more than thirty years’ experience, offers integrated security services for industry, tourism, trade, business, banking, mining and oil industries. It has 5,000 employees and the majority of its personnel have been recruited from the army.

VIMARCO LTDA is one of the companies that participated in founding BASC Colombia and the company became a certified BASC member in connection with the establishment of BASC in Cartagena de Indias in Colombia in 2001. The main reason for participating in the organisation was to prepare the company for being able to offer its customers security services that corresponded to their needs and market requirements. As a consequence of Colombia’s problem with drug smuggling there was a great need for competent security suppliers that could counteract these threats and risks.

Since VIMARCO is a company that offers security services the company has primarily invested money in the training of the guards, inspectors and other operative personnel that they send out to provide direct services for customers. The cost of this training amounts annually to approximately 10 million pesos. In addition to this, there are further costs of 1.5 million pesos for audit purposes and travel.

The greatest changes since certification in BASC have chiefly been in training and raising the awareness of its personnel. In addition to this, in order to gain the confidence of customers working with international trade activities, the company has developed a global vision with improved advisory services among the services it offers.

The greatest benefit since certification has been the positive development of its personnel. The personnel have been given training to meet the needs that exist in the international logistics chain and for this reason many customers have chosen this security company.

From the security perspective, certification has had the result that VIMARCO has been given instructions, training and has developed in the security field and, as a consequence of this, its work force has become more highly qualified. In addition it has been possible for the company to establish contacts with other certified security companies and in this way has been able to exchange experience and know-how. The investments made in further education and training and development of personnel in connection with certification in BASC have, according to VIMARCO, resulted in considerable benefits for the company.

The great change that has taken place since VIMARCO was certified in 2001 has principally been when the BASC programme’s version of security standards and norms was changed in 2005 and BASC, from having been an anti-smuggling alliance, became more of a company alliance for trade security.54

5.1.4 Members’ points of view

Researchers at the Cross-Border Research Association in Lausanne55 have made a case study of voluntary supply chain security programmes in which BASC was in focus. The aim of the study was to collect information on the costs of implementing and maintaining similar programmes and identifying the most effective security measures and the gains achieved.

In this case study an analysis was made of costs and benefits arising from BASC certification.

55 Gutiérrez et al. (2007).
The costs include expenditure arising from the implementation of the security measures themselves (security courses, investments in technology and buildings etc) and the annual administrative fees to the World BASC Organization. The latter vary from USD 800 till USD 2 000, depending on the socio-economic situation in the country of origin and the economic sector the company is part of.

Three categories of gains are listed in the study:

1. Direct security benefits
2. Benefits for the efficient functioning of the company under normal conditions
3. Benefits for the efficient functioning of the company under high alert or post-disaster conditions.

Since it is very difficult to make a quantitative assessment of any benefits of a programme such as BASC, the study chose to let respondents make their own assessments of the fields in which they had experienced benefits. Where the most and least important benefits are concerned, the respondents were rather unanimous: 70 per cent were of the opinion that the five most important benefits were improved company image and credibility; anti-smuggling; anti-theft; reduction in vulnerability in the supply chain, and improved supply chain performance. At the bottom of the list was a reduction in insurance premiums, which was in contrast to the anticipated high benefits in this area. The authors of the study assume that the reason why the premiums had not been reduced as expected is that the insurance companies, despite the significant security costs that accompany international trade transaction, do not regard BASC certification as an important criterion when premiums are determined.

According to the study, possible reasons why certain benefits did not correspond to expectations were that greater efforts are needed on the part of the companies to achieve these benefits, that certain security measures are not suitable for the achievement of the expected benefits, and that companies have not achieved these benefits since they have not been the subject of disruptions or crises where they could have demonstrated the effectiveness of the security measures.

Even if it is fully possible for the most part to calculate the costs of BASC certification it is, as mentioned above, very difficult to make a quantitative calculation of the benefits. This has the effect that it is not possible to make a detailed analysis of costs and benefits. Instead the study chose to ask the respondents on how many benefits, selected from a list, the company had achieved and how many security measures the company had introduced. One interesting result from the responses to this question was that it was not possible to determine any significant relationships between these two variables. Another calculation also shows that there is no significant relationship between costs and effectiveness among the security measures. Among the security measures that were considered effective there were just as many expensive as inexpensive measures, and the same applied to the ineffective measures.

The conclusions of the study was that BASC, despite certain specific problems, is a successful example of a private security initiative. According to the authors of the study it has become a well established organisation that promotes standards for security in the supply chain among its members. Above all, it is a successful programme from the perspective of the companies’ own routines and internal security. The companies that participated in the study experienced benefits in direct security that exceeded their expectations. At the same time the benefits in respect of cost reductions and facilitated border procedures were not as substantial as expected. Points of view presented by member companies refer to requests for state support for companies that participate in security programmes and stronger cooperation with local and international authorities. In addition it is mentioned that it is desirable to avoid a large number of programmes all over the world since this leads to a waste of effort and repeated information. The companies expect strong incentives from governments to participate in similar programmes, mainly in the form of special treatment at borders and tax reductions for investments in security.

6 Security programmes in Europe

After September 11, 2001, the European authorities have followed their American counterparts and presented a large number of proposals for security programmes:

- Rules for civil aviation security 2002,\(^{57}\)
- Enhancing ship and port facility security 2004\(^{58}\) and enhancing port security 2005,\(^{59}\)
- Amendment of the Community customs code and introduction of authorised economic operators (AEO) and 24-hour advance notification,\(^{60}\)
- Enhancing supply chain security,\(^{61}\) and

Customs issues are among the European Community’s core issues since the EC is basically a customs union but, in certain respects, the national customs authorities have considerable freedom to decide on their own implementation of the European customs policy. Despite this, only two countries in the EU, the Netherlands and Sweden, have drawn up partnership programmes between business and the customs authorities. However, these programmes came into being at an early stage – see the sections concerned. When the EU introduces common rules on authorised economic operators (AEO) in 2008 and regulations for their implementation are drawn up centrally by the Commission, this will represent a break with the earlier freedom in the system to some extent. It is a necessary arrangement in order not to put companies in any country at a disadvantage or to create other imbalances in the application of the rules. Sweden and the Netherlands will be obliged to make changes to adapt their systems to the common European model.

Rules for the advance notification of exports, imports and transit traffic will enter into force at the beginning of July 2009. They are more comprehensive than the corresponding legislation for imports to the USA and have been met with criticism from, among others, business associations for trade and wholesalers. A more detailed description is provided below of the preparations and the content of the legislation.

The EU rules can be divided into those which refer to traffic between the EU and third countries, and those that refer to traffic within the EU. The AEO system and advance notification refer to traffic between the EU and third countries. Where traffic within the EU is concerned, there is legislation in respect of the different types of transport: by air, road, rail and sea, and special rules for transport of dangerous goods, explosive substances and food. In connection to this the European Commission has taken initiatives to introduce legislation that will be common to all modes of transport and guarantee security in the supply chain.\(^{62}\) However, the proposal has not been well received by business associations\(^{63}\) and member states and is now dormant. As the Commission points out in its communication, it is a problem that there are no uniform rules for the entire land transport supply chain in Europe which complement the security rules that exist for other types of transport. Furthermore, the Commission intends to present new rules for air freight and for road transports of explosive substances.

---


\(^{62}\) Ibid.

\(^{63}\) See, for example, http://www.eurocommerce.be/content.aspx?PageId=40703
It can be predicted that developments in this field will remain in the focus of the debate on transports to and from Europe. In several cases the business organisations representing trade and industry have been dubious about the benefits of further regulation and point out the overlaps that exist within European legislation, and with other systems. At the same time the European legislators have the clear intention not to remain passive when faced with perceived threats to security and also intend to comply with the undertakings in the WCO’s SAFE Framework. On July 1, 2007, the EC, as an organisation, became an interim member of the WCO with full rights and obligations. In order for the EC to become a full member of the WCO it is necessary for WCO’s statutes to be changed to enable organisations to join.

6.1 The EU’s Customs Security Programme (CSP)

At the end of 2003, the Commission presented a proposal to the European Parliament and Council on measures to improve security in the supply chain. The proposal was adopted as a regulation of the European Parliament and Council amending Council Regulation (EEC) no. 2913/92 establishing the Community Customs Code. The regulation also presented a proposal to grant certain companies the status of authorised economic operator (AEO), which shall give them faster processing by customs authorities and other forms of trade facilitation, and the rules concerning the advance notification of both imports and exports of goods. The rules for AEOs enter into force on January 1, 2008, and the rules on advance notification on July 1, 2009. The measures are jointly referred to by the designation Customs Security Programme (CSP), which also includes jointly established control standards, risk indicators and greater cooperation between the customs authorities in the EU and other authorities in EU states, as well as with the authorities in the EU’s most important trade partner countries. In this context, the AEO programme shall be regarded as an effort to facilitate trade for legitimate operators. Furthermore, the amendments include a proposal that will give the EU a joint computerised risk assessment programme modelled on the USA’s electronic customs clearing environment, ACE, and risk assessment system, ATS.

A framework for risk assessment was introduced at the beginning of 2007 when the regulation (EC) no. 1875/2006 (in respect of implementation) entered into force.\(^{64}\) The aim is to achieve an equivalent level of security for the customs inspections that shall be performed when goods are brought into or taken out of the EU. The system shall be completely computerised in 2009.

In addition, the customs code shall also be changed in respect of a measure that is not related to security. The customs authorities in the EU shall be able to exchange export information electronically, which makes it possible for exporters to receive a receipt that a consignment has been exported immediately after it has left the EU. The system is called the Export Control System.

6.1.1 Authorised Economic Operators (AEO)

Article 5a in the modernised customs code contains the provisions that make it possible for customs authorities to grant AEO certificates to companies that have a background that guarantees the effectiveness of their control systems, their economic stability, and their capacity to observe existing customs rules. Once a company has been granted AEO status this status applies throughout the entire EU. A company that has received AEO status in a member state shall thus be recognised automatically by the other member states, but it does not give the company an immediate right to the customs facilitation procedures in force in other member states. However, other member states shall give AEO companies access to the facilitation procedures provided that they fulfil all special criteria for the procedure in question. This means that an AEO certified company that applies to be given a facilitated procedure shall only be examined on the basis of whether it fulfils the requirements that are linked to the facilitation in question and does not

---

have to repeat the certification process linked to AEO status. The common system is intended to contribute to creating an environment in which all companies in the community work under the same conditions.

The provisions in Regulation (EC) no. 1875/2006 on the requirements that shall be made of companies for them to be granted AEO status are detailed and provide little scope for supplementation or interpretation. AEO certificates are granted in the form of “AEO Certificate – Customs”, for operators wishing to benefit from simplifications provided under the customs rules (article 14a, 1a) or “AEO Certificate – Security and Safety”, for operators wishing to benefit from facilitations of customs controls relating to security and safety on entry and exit of goods (article 14a 1b) or AEO Certificate – Customs/Security and Safety which covers both fields (article 14a, 1c).

The regulation specifies in detail the country in which and the customs authority to which a company is able to apply for AEO certification. Likewise there are detailed provisions for those applicants that are not established in the community’s customs area but which are nevertheless entitled to apply. In the main this refers to companies that have AEO status in a country with which the EU has concluded an agreement on mutual approval of AEOs.

The requirement concerning compliance with customs requirements is considered fulfilled if the applicant company and the owners/main shareholders of the applicant company have been customs and/or fiscally compliant during the three years preceding the submission of the application. This may be assessed on the basis of the company’s customs declarations and the good faith of the applicant. If the company has been established for less than three years, the customs authorities may assess compliance on the basis of records and information available.

Furthermore, the regulation specifies detailed requirements in respect of the applicant company’s accounting system, its capacity to provide customs information and other reports physically and electronically, its capacity to distinguish between goods from the EU and imported goods, requirements for archival routines and IT security, etc. In addition there are brief rules for the assessment of a company’s financial solvency.

Article 14k contains a specification of the safety and security requirements that must be fulfilled. The security rules have been used in guidelines for AEO companies that have been the subject of a pilot project which has examined in detail how the requirements shall be implemented in practice and how it shall be possible to implement any possible advance examinations in order to avoid an excessive administrative burden when the system enters into force in January 2008. The security rules in the regulation are not as detailed as the security guidelines in the USA’s C-TPAT, but are nevertheless far-reaching. It should be noted that the security rules in C-TPAT more or less refer exclusively to one mode of transport, container traffic at sea, and to imports only. In this perspective the EU rules are more far-reaching since they refer to all modes of transport and both exports and imports. This has the effect that they must be formulated somewhat more flexibly.

It is of interest to follow the development of guidelines and provisions for the implementation of the regulation. There can be a risk that the implementation of the regulations will be different in different member states since the guidelines are not binding at the present time. The provisions refer to the appropriateness of premises, access control measures, and protection of goods – both to ensure that nothing is added to transports and to counteract any exchanges or losses of goods. Furthermore, it is laid down that the AEO companies must be able to identify their business partners. In this respect the provisions are less specific than the corresponding rules in C-TPAT. In addition, the ordinance includes provisions on security screening of personnel working in security-sensitive positions and on the training of personnel to enhance their security awareness.

Certification is intended to provide specific benefits. It is stated in the regulation that certification will result in an extensive reduction in the frequency of inspections, both document-based and physical inspections. The fact that controls performed in connection with AEO certification do not need to be repeated has already been mentioned above. AEO companies may use a simplified format for entry.
and exit summary declarations in connection with imports and exports, a right that also includes AEO certified carriers, freight forwarders and customs agents when they are acting on behalf of an AEO certified company. The information that must be provided within the framework of a summary declaration is specified in appendix 30a of the provisions for implementation of the regulation. Furthermore, the possibility is provided for customs authorities to contact an AEO certified company that has submitted an entry summary declaration to inform the company that the goods have been selected for additional security checks. However, the provisions do not mean that an AEO certified company is exempt from physical inspections; the customs always have the right to make such inspections, even without notifying the company, if notification would make the inspection more difficult to implement. An AEO certified company which is informed that a physical inspection of the goods will be made is, however, given the possibility to present a request in respect of the location of the physical inspection. Furthermore, the customs authorities can decide to increase the frequency of inspections with reference to a specific threat or any obligation to make inspections that derives from other EU legislation. Where the companies are concerned, misgivings have been expressed that facilitations in, for example, the submission of information in the entry and exit summary declarations are not sufficient to motivate the additional work that arises from AEO status. The interaction between AEO status and the 24-hour rule is regarded as being of decisive importance.

During the course of the process, the European Commission commissioned a test of the AEO model in a pilot project. The Commission’s website\(^65\) contains the results of the pilot study and the work that forms the foundation of the latest version of the AEO guidelines as well as guidelines for self-assessment of AEO status.

### 6.1.2 Rules for the advance notification of imports and exports

According to the European Commission’s regulation 1875/2006, the rules for advance notification have been introduced for both security and protection purposes. The companies will be liable to provide information in advance on both goods that shall be imported to and exported from the EU, and on transit goods.\(^66\) These entry and exit summary declarations are to be harmonised to make them identical throughout the EU. It will also be possible to process them electronically. It will only be possible to use paper forms in a few exceptional cases, principally when computer systems have broken down. No standard in respect of the electronic submission of information is given in the ordinance. This shall be drawn up by the Commission and the various customs authorities in agreement with each other (article 14x).

Today there are already requirements for importers and exporters for the submission of information (customs declaration) in advance for imports and exports that contain highly detailed information on the type of goods.\(^67\) These declarations will probably remain in place in the member states when the entry and exit summary declarations are introduced into the system, but will be made more flexible. For example, the introduction of summary declarations shall not lead to a double burden for companies. In cases where goods are included on a customs declaration, a further summary declaration is therefore not required. However, these customs declarations must contain at least the information required for summary declarations. This applies in particular to information that is relevant for security purposes.\(^68\)

A summary customs declaration shall be provided for goods that enter or leave the EU’s customs area. However, there are a number of exceptions to this rule and a specification of them is given in article 181c. This applies for example to electrical energy, goods that enter the EU via a pipeline, letters, cards and printed matter, personal baggage, etc.

---


Article 184a gives a number of time limits for the submission of entry declarations:

In the case of maritime traffic, containerised cargo shall be notified 24 hours prior to loading at the port of departure, and bulk and break bulk cargo at least four hours prior to arrival at the first port in the customs territory of the Community. For transports between a number of specified countries, over certain inland seas and from certain former colonies, the period of time is at least two hours. This applies to goods between Greenland, the Faeroe Islands, Ceuta, Melilla, Norway, Iceland or Morocco and the EU; between the French overseas departments, the Azores, Madeira and the Canary Islands and the EU if the duration of the voyage is less than 24 hours; and for movement from ports in the North Sea, Baltic Sea, Black Sea or Mediterranean to the EU. In the case of air traffic it is stated that if the flight is a short haul flight, i.e. a flight of less than four hours’ duration from departure in a non-EU country to arrival in the first airport in the EU, it is sufficient if the entry declaration is lodged at the customs office at least by the time of the actual take-off of the aircraft. Where long haul flights are concerned, the entry declaration shall have arrived at least four hours prior to arrival at the first airport in the EU. For rail and inland waters traffic, the entry summary declaration shall be lodged at the customs office of entry at least two hours prior to arrival and for road traffic at least one hour.

Regarding the exit summary declaration for goods transported by sea, the same time limits apply to exports as to imports. For air traffic the time limit is at least 30 minutes prior to departure from an airport in the customs territory of the Community and for rail and inland waters traffic at least two hours prior to departure from the customs office of exit. For road traffic the corresponding time limit is one hour.

The information that has to be submitted in the entry and exit summary declarations is relatively extensive. In addition to information on the consignor and consignee, information is also required in respect of the country/countries codes in route order and customs offices of exit, place of loading and unloading, commodity codes, description of goods, identification number of container and seal, method of payment code for transport charges etc. In particular the information relating to routes and ports of shipping is described by companies as difficult to complete since goods can often be redirected as a consequence of weather and port conditions. The requirements in respect of different types of codes has also be described as problematic, primarily for small and medium-size companies, since they can be difficult to obtain and mistakes can easily be made. The problems that can arise refer more to the difficulties for some operators to submit certain information and that the difficulty to submit information in time. A freight carrier has, for example, full control of information in respect of vessel and route, but must rely on information supplied by others where the goods are concerned. Where AEO companies are concerned, less information will be required in the declarations, but it is still a relatively small reduction: for an entry declaration it is a matter of a reduction of 29 possible items of information to 20.

6.2 EU rules for other modes of transport

In the EU there are a number of rules that are motivated for reasons of security. They mainly apply to transports within the EU and not to trade with third countries. Even if these rules refer, to some extent, to trade with third countries, for example, air transport, they have been collected under this general heading for the purpose of providing an overall picture.

6.2.1 Special rules for air freight

An annex to regulation 2320/2002 on the establishment of common rules in the field of civil aviation security contains the basic provisions that constitute the foundation of EU’s security

---

69 Some areas of Europe are not included in the customs territory of the Community. See text below.
70 Source: Swedish Trade Federation.
work in the field of air freight. The basic rule is that all parcels shall be physically checked, screened by x-ray equipment, and subjected to stimulation chamber or detection equipment for explosive substances.

Exceptions from the security controls may be made if the cargo comes from a so-called known consignor, is transshipment cargo, or can be guaranteed secure in some other way. Consignors can be designated as known consignors by regulated agents or air carriers, who have in turn been approved by the competent aviation authorities. Requirements in respect of a known consignor is that he prepares consignments in secure premises, uses reliable personnel, and protects the consignments against unauthorised interference during preparation, storage and transportation. In addition the freight forwarder must establish and register the identity of the consignors and the agents he uses, and require consignors to certify that consignments do not contain prohibited articles and to accept security examinations.

The regulation is currently being revised and, at the time of writing, a proposal has been processed by the Council. According to the proposal it will be necessary for aviation authorities to certify the known consignors. This will probably involve a cost for the consignors for the certification process and possibly differentiation in the handling of goods in order to show that it is beneficial to be a certified known consignor.

### 6.2.2 Special rules for maritime transport and ports

In March 2004 the EU adopted a regulation on enhancing ship and port facility security. This principally transfers the requirements from the international ISPS code into Community law. It has the effect that all measures in Part A of the ISPS code and parts of Part B are mandatory for the member states, while the remaining parts of Part B are only recommendations.

The rules for enhancing maritime security have the aim of protecting the maritime sector from intentional unlawful acts such as terrorism and are intended to ensure that suitable levels of shipping and port related security are provided as far as possible in all EU member states. This will be done by establishing and implementing community measures to improve maritime protection on ships that are used for international trade and national shipping. Preventive measures shall be taken, for example limiting access to port facilities and preventing weapons and dangerous substances being taken aboard ships or into port facilities.

The regulation contains provisions that each member state shall establish a competent authority for maritime security responsible for implementing the security inspections in ports. Security checks may also be performed by certain specifically selected inspectors. There are also provisions relating to 24 hour advance notification prior to a ship calling at a port, under which the ship is liable to provide the competent authority with security information. However, there are exceptions to the rules relating to the provision of security information.

The scope of the regulation is limited to security measures onboard ships and to collaboration between ships and ports. An amendment has therefore been added to the regulation in the form of a directive issued on enhancing port security. This directive has been produced with the aim of introducing port security measures in order to achieve the best possible protection for maritime and port operations.

A port is defined in the directive as any specified area of land and water that contains works and equipment designed to facilitate commercial maritime transport operations. Member states shall ensure that port security assessments are made before decisions are reached on the security measures that must be taken. The member states shall designate a port security authority for each port that shall be responsible for the preparation and implementation of port security plans, based

---


on the port security assessments. Furthermore, the member states shall introduce a system with three security levels. Level 1 is the level for which minimum protective security measures shall be maintained at all times. Level 2 is the level at which additional protective security measures shall be introduced at times of a heightened risk of a security incident. Finally, level 3 is the level at which further specific security measures shall be maintained at times when a security incident is expected or imminent.

6.2.3 Special rules for land transport and rail transport of dangerous goods

In the EU there is detailed legislation that prescribes how the transportation of dangerous goods shall take place. The basic provisions were drawn up in a UN agreement: European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR). This agreement has been implemented in the EU in two directives: the Council Directive 96/49/EC of July 23, 1996, on the approximation of the laws of the member states with regard to the transport of dangerous goods by rail and the Council Directive 94/55/EC of November 21, 1994, on the approximation of the laws of member states with regard to the transport of dangerous goods by road, with appendices. The rules include, among other things, provisions relating to controls of the carrier’s identity; protection and lighting at marshalling points and terminals, and the training of drivers. Moreover, it is stated in the provisions that carriers, consignors and others handling dangerous goods with a high risk potential shall introduce safety plans that, among other things, specify the risks relating to infringements of the protection of dangerous goods.

Furthermore, the Commission has presented a proposal on new rules for the transportation of explosive substances.74

6.2.4 Proposal to enhance supply chain security – Secure Operator

In February 2006 the European Commission presented a proposal for a regulation that would enhance supply chain security – also known as the Secure Operator proposal.75 The basis of the proposal is that each operator in the supply chain shall be responsible for his own security and in this way the security of the entire chain is guaranteed. All operators in the different member states shall be able to show that they fulfil the legal requirements in respect of security in a programme for secure operators. It shall be possible to give these operators facilitations in security controls. According to the European Commission, the objective of the proposal is to “increase the level of security along the supply chain without impeding the free flow of trade”. The proposal was withdrawn by the Commission after its first reading in the European Parliament after it had received massive criticism from European business associations such as Clecat and Eurocommerce.76

6.3 Sweden: Stairway and StairSec

Since 2002 the Swedish Customs has used a quality assurance programme for companies. The programme is called Stairway. It has been designed to ensure efficiency, quality and safety in third country trade by encouraging compliance with rules and offering facilitations. One foundation for this work is a positive climate of cooperation between the Swedish Customs and the Swedish companies. Stairway was produced between 1998 and 2002. Development work was carried out in cooperation with trade and industry and fifty companies participated in pilot studies which preceded the final programme. At the same time this work has also been part of a European development project, COMPACT, together with the Netherlands, and Sweden has worked actively to have the Swedish model for quality accreditation approved internationally.

75 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, COM(2006)79 final.
All companies that do trade with third countries are included in Stairway but are on different steps in the programme depending on whether their customs routines have been the subject of quality assurance or not. Quality assurance in Stairway means that the Swedish Customs, after implementing a quality assurance process of companies’ routines, can certify the companies for simpler and more efficient customs handling. An examination is made of the companies’ operations and routines. The routines shall ensure that the information submitted by a company is correct from the outset and the company is then given faster and smoother customs treatment. The principle is that the better the knowledge Swedish Customs have of a company’s flow of goods and information, the more facilitations the company can be given in customs clearance and thereby reduce the risk of disruptions in the company’s flow of goods. Use is made of the information in the companies’ business systems and the companies are given solutions and facilitations adapted to the customs processing of each company. One prerequisite for being certified in Stairway is that a company’s goods declarations can be submitted electronically, either via the Swedish Customs Internet declaration, which is available on the Swedish Customs’ website www.tullverket.se, or via EDI/EDIFACT from the company’s business system (see figure 6.1).

In the programme it is possible to certify parts of a company. However, this possibility will disappear when AEO certification replaces the higher certification levels in Stairway.

One possible simplification is the so-called local clearance procedure which means that, instead of requesting a customs declaration, the Swedish Customs approve the information in the business system when the goods are received and checked by the company, or made ready for shipping. This system has the effect that it is not necessary to contact the Swedish Customs for each individual import or export, but rather that a supplementary electronic customs declaration is submitted at a later point in time.

During the quality assurance process, an officer from the Swedish Customs is appointed as the contact person for each participating company. After the quality assurance process, this officer continues to help the company with its customs administration and is also responsible for the regular follow-up of the company.

Fact box 6.1 The Swedish Customs’ Stairway. All companies are included in Stairway but to reach steps 3-5 they must be accredited.
To minimise security risks in the supply chain, Stairway was extended with a new module in 2003: Stairsec (Stairway Security Programme). Companies that are accredited on levels 3-5 in Stairway can apply for accreditation in Stairsec. During the quality assurance process for Stairsec, the companies’ operations, flows of goods and security awareness are initially surveyed with the aid of a questionnaire for accreditation purposes. In this connection, the company examines its routines and ensures that everything is documented before an application is made to Stairway. The use of a questionnaire ensures that the accreditation process is uniform and that the same level of quality is maintained for all companies. In the next step the Swedish Customs works together with the company to establish priorities and evaluate different risks in the company’s operations and flows of goods. The accreditation process in respect of security includes the following areas: all its facilities, the logistical flow, staff and the operators in this flow, IT systems, and the flows of information between the company and its external partners.

Since they constitute a smaller risk of being used for illegal purposes, companies that are accredited in Stairsec are subjected to fewer controls. Linking Stairsec to facilitations in Stairway was a deliberate method to create incentives for companies to participate in StairSec. It was also made easy since it linked up to an already existing concept.

In Stairsec there are four different modules that focus on different roles in the supply chain:

- Operators (importers and exporters)
- Customs brokers and agents
- Transporters, freight forwarders and carriers
- Terminals and ports

According to the Swedish Customs, one requirement in the development of StairSec was that the system should comply with the requirements made by other international security systems such as C-TPAT and CSI. Representatives of the American customs visited Sweden in 2001 and studied Stairway and it is obvious that there are considerable similarities in the thinking behind Stairway (at that time Stairway did not have a security module) and C-TPAT, even if C-TPAT only focuses on security. According to the Swedish Customs, Stairway together with its security module, StairSec, corresponds entirely to the AEO certification that was introduced at the EU level on January 1, 2008, in respect of the criteria an operators must fulfil in order to be given AEO status.

### 6.4 Quality assurance in the Netherlands

#### 6.4.1 Dutch Client System

In common with the Swedish Customs, the Dutch Customs has a programme that focuses on assessing the reliability of companies on the basis of the way in which they administer their customs routines from a risk analysis perspective. The programme is called the Dutch Client System. It has been mainly used internally by the Dutch Customs rather than vis-à-vis companies. It has been developed on the basis of two fundamental concepts: that goods themselves do not commit fraud and that compliance with rules should be promoted. Due to the Netherlands’ unique position as a trading country, the Dutch Customs have experienced a considerable need to respond to the logistic procedures developed by trade and industry and has chosen to use solutions adapted to the ways in which companies and sectors themselves handle their risks. This approach makes it possible to draw up a control programme adapted to each company. The most important components in the Dutch concept are:

- Preliminary review – the first stage to determine the most suitable arrangement for the company concerned and to examine whether or not an authorisation may be granted.

- Control programme – a directive in which the type, frequency and scope of the ideal means and methods of control to be used are laid down per client, using the knowledge of that client, risk analysis and tailor-made regulations.
• Treatment plan – a document that lays down those elements of the control programme that will actually be implemented in light of available capacity.

In addition to this the working team that works with the company – the client – has certain definite roles:

• Team leader – responsible for the team that takes all the necessary measures to determine whether or not an authorisation shall be granted and which elements of a control programme are supposed to be implemented, to draw up treatment plans and to direct the controls.

• Client coordinator – responsible for collecting and analysing information on “his” clients, for performing risk analyses and drawing up control programmes for each of those clients, and for bearing the responsibility for integral treatment of clients.

• Auditor – responsible for preliminary reviews of potential clients and for audits of books and records of existing clients.

In the main it is the major companies that can count on completely individualised treatment in respect of risk analysis and systematic work on risks. Other companies are classified in groups based on the types of goods they work with. In common with the Swedish programme, Stairway, the clients are divided into five groups based on the complexity of their accreditation. 

In the accreditation work done by the Dutch customs, consideration is given to the company’s organisation and accounts and data on the company’s processes for its activities and customs procedures. Furthermore, an attempt is made to identify strengths and weaknesses in the internal control at the company.

The Dutch Customs states on its website that it is possible to apply for AEO status from September 2007. It is unknown how their programmes will be adapted to AEO but it is probable that the same procedures will form the basis of AEO certification.

6.4.2 PROTECT

On January 1, 2005, a four-year project was started which had the goal of developing reliable supply chains. Protecting people, planet and profit, PROTECT in brief, is a programme of cooperation between, among others, the Dutch customs and the Port of Rotterdam. The goal of PROTECT is to identify the factors that determine the level of reliability and security in national and international supply chains and how companies and governments can influence these factors to secure the supply chains. In 2006, PROTECT focused on the development of knowledge in respect of exchange of information in logistical chains.

6.5 Cooperation between the USA and EU in security matters

In 1997 the EU and the USA signed an agreement on customs cooperation and mutual assistance in customs matters. In the agreement a framework is provided for customs cooperation and, with this as the point of departure, a customs cooperation committee was established by the EU and the USA, the EU-U.S. Joint Customs Cooperation Committee (EC-U.S. JCCC). In April 2004, the EU and USA signed an agreement on more intensive cooperation in security matters, for example on CSI and other security initiatives. The point of departure is that the EU and the USA have a common interest in performing as high a number of controls as possible without hindering trade – that work should focus on high risk objects. Two expert groups were appointed: the Security Standards Group and the Trade Partnership Group. They have worked on furthering joint efforts in respect of security standards, and on the mutual recognition of accreditation programmes. The recommendations arrived at by the expert groups constituted the substance of the list of measures that were agreed at the 7th meeting of the EU-U.S. Joint Customs Cooperation Committee in Brussels in January 2006. The groups of experts were transformed into a steering group and it is currently processing the measures which include, for example, a comparison between the EU’s AEO and the USA’s C-TPAT. The nine measures are:
1. Minimum requirements for EU’s feeder ports to CSI
2. Pilot project on transshipment
3. Exchange of information
4. Risk rules
5. Temporary posting of EU liaison officer(s) at the National Targeting Center
6. Common list of advance cargo data elements
7. Research and development issues
8. Joint threat assessment

Draft conclusions for certain measures were presented in January 2007 and the work is continuing.

The transatlantic dialogue was formalised in April 2007 at a meeting between President Bush and Chancellor Merkel when an agreement was reached on a framework for strengthened transatlantic integration and the Transatlantic Economic Council (TEC) was established. The Council, which intends to meet every sixth month, is led by the Assistant to the President of the USA for Economic Policy, Daniel Price, and the European Commission’s Commissioner for Enterprise and Industry, Günter Verheugen. At a meeting in the beginning of November 2007, agreement was reached on a plan to mutually recognise the EU’s AEO programme and the USA’s C-TPAT programme in 2009.
7 Security initiatives in Asia and Oceania

In Asia and Oceania there are supply chain certification programmes corresponding to C-TPAT or AEO, currently mainly in Australia and New Zealand, which are developing their programmes to comply with the WCO’s definition of AEO. In Asia there are few examples of certification programmes hitherto. As a consequence of the lack of initiatives of this type work is currently being done on different fronts to enhance security in the supply chain both through national programmes and regional cooperation. One common factor in these programmes is that there is no certification; it is rather a case of general guidelines for security in transport and travel. Another common factor is that preparations are being made for the WCO’s SAFE framework with the aid of these initiatives (see separate chapter).

7.1 APEC/STAR

Asia Pacific Economic Cooperation (APEC) is an economic forum for countries around the Pacific Ocean. The member states discuss matters that concern the regional economy, cooperation, trade and investments. All in all these states represent 60 per cent of the world’s GNP and 46 per cent of world trade. APEC was originally an Australian initiative, produced in 1989, which focused on the liberalisation of trade and investments, promotion of business, and economic and technical cooperation.

Where the theme of security for transport and travel is concerned, APEC has arranged the so-called STAR conferences (STAR – Secure Trade in the APEC region) since 2003. The conference in 2007, STAR V, was held in Australia in June and focused on cost-effective solutions to enhance security in travel and transport in the region. STAR is an initiative which, in common with C-TPAT and CSI, was created as a reaction to the terrorist attacks of September 11, 2001. The heads of government in the APEC states have therefore created an action plan which aims to enhance security for goods, ships, aircraft and passengers with the aid of a number of security measures. These measures shall be implemented in the fields listed in the fact box below.

Fact box 7.1 APEC’s Supply Chain Security Guidelines

In the action plan for STAR mentioned above, it is recommended that companies, in accordance with their own needs, comply with these security measures, and comply with international standards and requirements laid down by the WCO, IMO, ISO etc. However, no movement towards certification in the field of security in the supply chain within the framework of APEC can be discerned at the present time.

The USA is playing an important role in this programme of cooperation and has succeeded in introducing the Container Security Initiative (see section on USA) in most major ports in the region. Furthermore, the USA has been the driving force behind APEC’s action plan.

---

77 APEC’s member states are Australia, Brunei, Chile, the Philippines, Hong Kong, Indonesia, Japan, Canada, China, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Russia, Singapore, South Korea, Thailand, USA and Vietnam.

7.2 EU – China: Smart and Secure Trade Lane Pilot Project

In 2005 the EU and China concluded an agreement on customs cooperation and mutual customs assistance. This agreement was consolidated in 2006 when it became a pilot project on security in the supply chain. The project was named the Smart and Secure Trade Lane Pilot Project. The motive for the agreement in 2005 was to combat counterfeit goods and pirated goods, all of which constitute a growing threat to trade between the EU and China, as well as terrorism. In addition, it is probable that authorities in the EU and China want to ensure that they can meet the requirements stipulated in C-TPAT. By strengthening customs cooperation between the parties, trade will be facilitated while problems are combated. The goal is to create smart and secure trade routes which initially include the ports of Rotterdam in the Netherlands, Felixstowe in Great Britain and Shenzhen in China. At the present time, the project is a cooperation project between the EU Commission, the customs authority in China and the customs authorities in Great Britain and the Netherlands. If the project is successful it will be gradually extended to cover the entire EU as well as more ports in China.

Both sides agreed to exchange experiences and develop routines in order to better understand and prepare the implementation of the WCO SAFE framework (see separate chapter). It was also decided that the parties would work towards greater mutual recognition of security measures by the customs authorities in China and the EU.

In the short term the Smart and Secure Trade Lane Pilot Project will permit tests of “end to end supply chains” from the point in time when a container is loaded through its entire journey up to its final destination. There is also the ambition to reach an agreement on common criteria for AEO status. Common requirements in respect of certificates that security controls have been implemented before a container is filled is another ambition in the short term, as well as a joint definition of minimum risks and minimum standards for controls and certificates of customs controls. Finally, an examination and evaluation shall be made of IT and other technical solutions which improve security and control systems, at the same time as legitimate trade will be facilitated.

In the long term the project is expected to lead to mutual recognition of security standards, control results and AEO programmes. The latest technology shall be used to secure the supply chain and there is an intention to improve the flows of information and risk assessments, and to raise the level of the objectives of controls. As a result of the project it will be possible to unload goods faster on arrival. At the same time the predictability of delivery times will improve and fewer resources will be needed for control of AEOs.

7.3 Australia

Australia’s policy for security in the supply chain is reminiscent of Canada’s since it is based on voluntary cooperation between the customs administration and companies and since its main focus is on the exchange of information. At the present time the Australian Customs Service (Australian Customs) is implementing a pilot AEO project which demonstrates Australia’s ambition to fulfil the rules laid down by the WCO and that Australia is thus approaching the thinking of the USA and the EU in this field.

7.3.1 Frontline

In 1991 the Australian Customs started a programme of cooperation with companies in the country which had the aim of enhancing security in the supply chain. The point of departure of the programme, which is called Frontline, is that companies sign a Memorandum of Understanding (MOU) with the Australian Customs. In the MOU the company and the customs show their intention of cooperating against illegal activities such as weapons smuggling, terrorism, trafficking in humans, drug trafficking, and wildlife smuggling. It is an agreement which, even if it is not legally binding, formalises cooperation between the parties that have signed it. By signing
a MOU, a company agrees to provide the customs with timely information about suspicious incidents, to develop its cooperation with the customs, and to continually check and improve its internal security arrangements. In return the customs will, as far as possible, make it easier for the company to conduct its business operations. The customs will also offer training and advice in matters concerning security and drug prohibition, and encourage and participate in the development of cooperation arrangements.

According to the Australian customs, Frontline is a programme that is based on trust and the dissemination of information. As opposed to C-TPAT and CSI, which are both security initiatives that have been created to strengthen security in container traffic in practice, Frontline focuses, in common with Partnership in Protection – PIP (see section on Canada), on preventing illegal imports and exports through the collection of information from partner companies. These companies function as the external eyes and ears of the customs. To enable companies to make a reasonable assessment of whether an incident is suspicious or not, the Australian Customs has published a number of indicator sheets which all participants in the programme have access to. These sheets present a number of questions which are intended to assist the companies in their assessments, and include activities in respect of air traffic, goods transportation, wharfs, container handling, ships on international journeys, and customs clearance procedures.

Membership is free and in the autumn of 2007 there were some 700 member companies. Companies that are involved in international trade and transport can become members of Frontline. According to the Australian Customs, this programme of cooperation has led to many successful crime investigations. In 2006-2007 every fifth notification of a suspected crime received from a member company led to a positive outcome for the Australian Customs.

To improve the discovery of illegal drugs, the Frontline Enhancement programme was started in October 2006. Within the framework of this programme the Australian Customs has tested a number of strategies aimed at encouraging greater participation on the part of Australian companies.

7.3.2 Authorised Economic Operator (AEO)

In July 2006, the Australian Customs started its Customs to Business partnership model, which is a pilot project for security in the supply chain, and has purpose of introducing Authorised Economic Operator (AEO) status for companies. Companies that wish to be granted this status must introduce a security system which fulfils the minimum requirements in respect of security laid down in WCO’s SAFE framework (see below in this section). The system shall also meet the requirements laid down in C-TPAT and New Zealand’s Secure Exports Scheme. Among other things, requirements are stipulated in respect of relations with third parties, personnel policies, transport, IT and information, as well as container security. If the company fulfils these requirements its supply chain undergoes a number of controls. If it is assessed that the company is suitable to be granted AEO status, it can sign an agreement with the Australian Customs.

With the aid of the pilot project, the Australian Customs wants to test and finely tune application and assessment procedures for the accreditation of different types of companies in the supply chain as AEOs. Furthermore, the Australian Customs wants to design a system that will have the result that AEO status in Australia can lead to recognition by customs authorities in other countries.

The Customs to Business partnership model is still in its pilot phase and only five companies are participating in the project. The Australian Customs is of the opinion that with the aid of this project it will be possible to show the country’s engagement in matters that concern security in the supply chain, and the project was presented during the STAR V conference that was held under the auspices of APEC (see separate section) in Australia in June 2007.
7.4 New Zealand - Secure Exports Scheme

In common with Australia, New Zealand has a programme of cooperation between its Customs Service and companies in respect of security measures in the supply chain. It is a voluntary-based initiative that is called the Secure Exports Scheme. According to the New Zealand Customs Service it is open to all exporters to all destinations.\(^7^9\)

The initiative is a partnership with a standard procedure for companies that choose to participate. The companies undertake to take security measures together with the New Zealand government, represented by the Customs Service. Based on a company’s security plan, which must comply with the Customs Service’s security principles and include existing security measures, participation in the Secure Exports Scheme is formalised. At the same time, the New Zealand government is trying to minimise bureaucracy and costs relating to the fulfilment of the requirements in order to make it easier for trade.

By signing a partnership agreement with the Customs Service, companies undertake to ensure that goods exported from New Zealand under this initiative are packed securely. The companies must have satisfactory routines to ensure the security of the goods and the goods must be transported securely without disruptions at the place of shipment. Containers or other packages that are transported by sea must be secured with a seal or other types of marks approved by the customs service, which signifies that they are under customs control and can be regarded as being secure by customs authorities in other countries. The companies undertake to guarantee that the contents of the containers are reported carefully and that nothing has been added to the cargo. The companies are expected to submit precise export information in advance, maintain a high level of security, and show the will to cooperate. By giving a greater guarantee in respect of their exports, the companies that are partners in the Secure Exports Scheme experience less involvement on the part of the customs in their export activities, according to the New Zealand Customs Service.

According to the New Zealand Customs Service, partnership will lead to a number of benefits for the companies. Supply chains are secured from packing to loading for export, and charges for the storage of export goods will be lower, for example due to the fact that the companies are given so-called “green lane” status, which means that cargo can be moved to a port or airport with little likelihood of customs controls. Furthermore, the companies will experience improvements in contacts with foreign customers and customs authorities. By entering into partnership, companies show to foreign importers that they fulfil certain standards, at the same time as customs clearance in the USA is facilitated if the customer is certified in C-TPAT. Moreover, companies will probably experience few problems with disruptions in exports as a result of heightened levels of security preparedness, since their security status can be certified. The New Zealand Customs Service can offer companies advisory services if the companies encounter unexpected problems with their export goods at other countries’ borders. Through partnership the partner companies implement security measures that follow the WCO’s framework for secure trade.

7.5 Singapore – Secure Trade Partnership (STP)

Its position at the south-east entrance to the Strait of Malacca makes Singapore a very important port strategically since the Strait of Malacca is the main passage between the Indian Ocean and the Pacific Ocean. Some 50 000 ships pass through the Strait of Malacca each year and these ships carry between a quarter and a fifth of all world trade at sea. Calculated on the basis of the number of containers received, Singapore was the world’s largest port in 2006.\(^8^0\)

A quarter of all oil maritime transports passed through the Strait in 2003 which, at the Phillips Canal, narrows to a mere 2.8 km. For hundreds of years its geographical position has attracted


pirates, a problem which has grown during recent years and which has led to greater cooperation between the coast guard administrations in Singapore, Malaysia and Indonesia. The fact that four-fifths of the container traffic to Singapore consists of transshipments reinforces the effect on world trade if a terrorist attack should occur. This, in combination with the country’s vulnerable geopolitical situation,\(^1\) has led to greater consideration being given to security with the emphasis on threats from terrorists, and close cooperation with the USA. This is reflected in the country’s security strategy for maritime traffic. Singapore was the first country in Asia that signed a CSI agreement with the USA.

On May 25, 2007, the customs administration in Singapore launched the Secure Trade Partnership (STP), a voluntary certification programme which, in common with corresponding initiatives in Australia and New Zealand, is intended to encourage companies to introduce security measures in their operations in order to enhance security in the global supply chain. According to the Singapore customs, STP is consistent with the WCO’s SAFE Framework. The customs emphasise that the idea behind STP is not that it shall replace other security initiatives that companies may have introduced. Even if other initiatives cannot replace STP, the customs will take into consideration existing certificates that the companies have received, provided that the requirements in these overlap the requirements in STP.

With the aid of this programme the customs wishes to underline the importance of having a holistic view of security in the supply chain. Companies are encouraged to adopt an active role in the work of making Singapore a secure hub in international trade. This will be achieved by companies following a framework in which they develop, implement, check and review their security measures and routines. Interested parties in the international supply chain such as importers, exporters, warehouse operators, freight forwarders, terminal operators etc are welcome to participate in STP according to the Customs. By being accredited in STP, companies will have better transparency in their supply chains and thus a reduction in their losses from theft. In addition, they shall undergo fewer goods inspections since they are recognised as low risk companies, both in Singapore and in other countries.

In order to obtain STP certification, a company must evaluate its internal policy, processes and procedures and compare them with STP’s guidelines. The evaluation shall include the company’s security management system, its risk assessment process, and the security measures that correspond to STP’s guidelines. See fact box 7.2 below.

---

**Fact box 7.2 Guidelines for the Secure Trade Partnership (STP)**

Source: [www.customs.gov.sg](http://www.customs.gov.sg)

- Premise security and access controls
- Personnel security
- Business partner security
- Cargo security
- Conveyance security
- IT security
- Incident management and investigations
- Crisis management and incident recovery

---

\(^1\) Goh (2005) points out that Singapore’s geographical position has led to two main security concerns. One is Islamic influences from its neighbouring countries Malaysia and Indonesia. This potential threat has been further reinforced since the attacks against the USA on September 11, 2001, and a comprehensive anti-terrorist programme has been produced. The second threat, which has more of a long-term character, comes from China whose strengthened role, both economic and military, carries the risk of destabilising the political situation in the region. In the opinion of Goh, Singapore is protecting itself against both threats through close cooperation with the USA.
If a comparison is made between STP’s and APEC’s guidelines it is clear that they are based on the same basic concept of security in the supply chain. The similarities also extend to ways in which the programmes relate to the WCO’s SAFE Framework. Both programmes are voluntary and Singapore Customs has, like APEC, expressed its support for accreditation in other programmes that are intended to enhance security in the supply chain.

7.6 Jordan – the Golden List Program

The Golden List Program was started in Jordan in 2005. It is a programme that has the aim of securing the supply chain. One important idea behind the programme is to attract foreign investors by creating a more secure investment climate. It is based on risk management and compliance with customs requirements, and international security standards. Companies that are active in importing, exporting, customs clearance, transport management or warehousing, and so-called Qualified Industrial Zone (QIZ) companies, shall, if they fulfil customs requirements for a Golden List company, enjoy a large number of benefits in the form of simplified routines. In order to be approved for the Golden List, a company must, among other things, have a sufficiently large trade volume, have an acceptable compliance rate in its customs declarations during the year prior to application, have not been the subject of litigation with the customs, and have been active for a certain period of time before it can apply. It must also have introduced and followed certain security measures. Even if the initial trial period of the Golden List Program is over, it is still in its pilot phase and only 15 companies are participating in the programme.

---

82 In 1996 the President of the USA Bill Clinton, concluded an agreement with Jordan on so-called Qualified Industrial Zone companies. These companies are exempted from customs duties and quotas on their exports to the USA.
8 Private cooperation initiatives

There are two major private cooperation initiatives for security in the supply chain that have been initiated by companies to rectify security problems related to international trade and transport. One, BASC, has been discussed in a separate section above on account of its strong links to C-TPAT and its regional links. The other initiative is the Transported Asset Protection Association (TAPA). While BASC came into existence as a response to drug smuggling, TAPA is an initiative that has mainly come into being to reduce losses that arise through theft in the supply chain.

8.1 Transported Asset Protection Association (TAPA)

The Transported Asset Protection Association (TAPA) is an international association for manufacturers and freight carriers which cooperate to counteract the growing threat to security. TAPA is a non-profit association which was formed in the USA in 1997 and which started working in Europe in 1999 and in Asia in 2000. During the 1990s there was a pronounced increase in cross-border crime in the EU. TAPA links this to the introduction of the EU’s inner market which, according to TAPA, made it easier for criminal gangs to move across borders. According to TAPA EMEA (TAPA Europe, Middle East and Africa), this is not just a case of smuggling drugs and people, it also includes crime directed towards transports of goods with a high value.

TAPA’s overall goal is to identify the fields in which members experience losses, and to share information on effective routines and practices. TAPA’s main target group is companies that are active in the production and transport of high-value goods. As opposed to most other security initiatives in the supply chain, TAPA’s security measures focus on truck transports and do not take up container transports at sea at all. Another distinguishing feature of TAPA is its exclusive image. Since the programme focuses in its entirety on the transport of high-tech goods, the possibility to become a member of the programme is strictly limited for an average company. Initially, only companies that produce or export high tech goods could become members, but this was later extended to include companies producing other high value goods.

Membership

There are four levels of membership in TAPA: full membership, associate membership, TAPA associated partner (TAP), and honorary membership. Membership is approved by TAPA EMEA Management Committee. Companies with full membership include Apple, Dell, Intel, Microsoft and Volvo. Companies with associate membership include DHL Express, Maersk Logistics and the Swedish Mail Service (Posten).

Security initiatives

When TAPA was established two main initiatives were introduced: Incident Information Service (IIS) and Freight Suppliers Minimum Security Requirements (FSR). IIS is a service for the exchange of security-related information that TAPA provides for its members. FSR are requirements that are placed on general security in the supply chain and which include, among other things, external security, premises and security routines.

8.1.1 Exchange of Information/Incident Information Service (IIS)

The Incident Information Service (IIS) is an initiative that has been devised by the members themselves. It is a form of cooperation that is based on the exchange of information on criminality associated with the supply chain of high-tech products. The information flows take place in industry and between industry and law enforcement agencies or the like. IIS has now been extended to include other high value freight. The idea behind IIS is to create a centralised...
information bank on criminality against freight in transit in the EMEA region and to facilitate the dissemination of this information to member companies and law enforcement agencies.

According to TAPA, the benefits derived from IIS are that the rapid dissemination of information about an incident is facilitated, which in turn facilitates investigations and the recovery of stolen goods. Furthermore, TAPA points out that IIS makes well-based statistical analyses of problem areas possible, which facilitates preventive action. Increased awareness of problems relating to cargo theft at the local, national and international level is another advantage of the service.

Within the framework of the programme, TAPA members are offered Flash e-mail Incident Event Notifications, a service which, according to TAPA, rapidly spreads information on new incidents. IIS also includes a database of all incidents experienced by members. The database is available to both member companies and law enforcement agencies. The members are included in a contact network which has the form of a member and cooperation directory in which law enforcement agencies, companies and logistics security personnel are listed. Investigations of incidents are further facilitated as a result of a register of links to the product descriptions of the manufacturing companies. Finally, the members receive a monthly bulletin in which the latest incidents are summarised and an analysis of important data is presented.

8.1.2 Freight Suppliers Minimum Security Requirements - FSR

Requirements that the member companies must meet to be certified in the Freight Suppliers Minimum Security Requirements (FSR) programme is strongly linked to buildings and routines and, as opposed to most other security initiatives in the supply chain, personnel matters are given very little attention. External security is a field in which the security measures are highly reminiscent of both BASC and C-TPAT. External physical barriers, as well as lighting, CCTV surveillance and intruder alarm systems are regulated under this heading.

FSR also contains requirements in respect of indoor security. Routines for entering and leaving office areas will be introduced. Restrictions in respect of access to docks and warehouses, and routines for vaults and storage are examples of requirements of this type.

The member companies shall introduce security systems that include surveillance systems, routines for the registration and retention of CCTV recordings, maintenance of alarm systems etc. Documentation and reporting procedures as well as an effective report chain for emergencies shall be established. Other examples of security procedures are the regulations concerning ways in which employees and visitors shall carry ID badges, and routines when personnel leave the company permanently.

Where security during truck transport is concerned, there are a number of standard requirements in FSR. These take up both practical and procedural aspects of security such as the installation of security devices on trucks, communication systems and routines for scheduling routes and loading/unloading of cargo. Transports of goods shall be notified prior to arrival. There are also requirements in respect of training for drivers, escorts of truck transports and GPS vehicle tracking. The main features of TAPA FSR are summarised in fact box 8.1 on the next page.
A study commissioned by TAPA\textsuperscript{84} showed that considerable savings could be made by companies working in the fields of high technology, pharmaceuticals, and the sale and manufacture of high value goods through this form of cooperation. According to the study, the average member company had reduced its losses due to theft by more than 40 per cent as a result of having a supply chain certified through FSR.

However, at the same time as theft during the storage of goods has decreased considerably, thefts during truck transports have increased drastically. In Great Britain, for example, the number of truck hijackings increased by 200 per cent during the first six months of 2006 compared to the same period in 2005.\textsuperscript{85} According to Eurowatch, the thefts that occur during truck transports constitute 86 per cent of all thefts in the supply chain. As a reaction to this problem the Freight Supplier Minimum Trucking Security Requirements (TSR) were introduced in 2006.

### 8.1.3 Freight Supplier Minimum Trucking Security Requirements (TSR)

As opposed to the more general character of the FSR criteria, TAPA’s Freight Supplier Minimum Trucking Security Requirements (TSR) are directed specifically at the transport of goods by truck. TSR identifies minimum acceptable standards for security throughout the entire truck-based

---

\textsuperscript{84} Purtell (2007).

supply chain and methods for the introduction of these standards. The requirements for security measures within the framework of TSR include a truck transport in its entirety, from loading to unloading. One interesting difference from FSR is that it has been decided that personnel security should be emphasised as an important aspect.

In TSR companies are given directions for ways in which trucks and trailers shall be equipped with, for example, locks and seals. Companies shall also install communication and tracking equipment such as radio and satellite tracking systems, as well as alarm systems and equipment to secure trucks when they are standing still.

Purely procedural aspects of security in truck transport are, among other things, rules for procedures to be used for the documentation of deliveries and sealing of trucks. Other points are the advance notification of information, scheduled routes, reports and programmes for vehicle maintenance etc.

Where personnel are concerned, emphasis is given to the importance of checking the background of employees and that companies should establish procedures for ways in which personnel are employed and how they leave the company. The security awareness of employees shall be enhanced, among other things they shall be prepared for robberies in the form of robbery response training. Another personnel-related security matter is the need of double drivers on risk full routes, and escorts of truck transports. The main features of TAPA TSR are summarised in fact box 8.2 below.

---

**Fact box 8.2 Main features of TAPA's Freight Suppliers Minimum Trucking Security Requirements (TSR)**

- **Physical security**
  - Truck security
  - Trailer security

- **Security systems**
  - Communications
  - Tracking and tracing
  - Alarm
  - Vehicle immobilisation

- **Security procedures**
  - Collection of information
  - Delivery
  - Pre-alerts
  - Scheduled routing
  - Incident, event and action reporting
  - Vehicle maintenance programme
  - Stops
  - Secure parking
  - Contingency planning
  - Key management
  - Unauthorised persons

- **Personnel security**
  - Screening/vetting
  - Pre-employment checks
  - Hiring and termination procedures

- **Training**
  - Security awareness
  - Robbery response training

- **Enhanced security requirements**
  - Drivers
  - Truck escorts
COMPANY EXPERIENCE: TNT

TNT offers companies and consumers international express and mail services. TNT Express, which is a part of the group, is one of the world’s largest business-to-business express transport operators. With its head office in Holland, TNT offers network structures in Europe and Asia. TNT is located in more than 200 countries and has some 159,000 employees. In 2006 TNT reported earnings of EUR 10.1 billion. TNT is listed on the stock exchanges in Amsterdam and New York.  

TNT is an associate member of TAPA. Since TNT has the very largest manufacturers of technology as clients, security considerations are of utmost importance in its sector and are the reason why it decided to join TAPA. The cost of certification (i.e. the costs of investments in security equipment) was in round figures SEK 1.5 million per terminal. Since TNT had introduced a security philosophy internally prior to joining TAPA, only minor adjustments were required to achieve TAPA’s standard conditions for certification. In addition TNT has many security requirements imposed by aviation authorities (since it also has air transports).

The advantages of membership in TAPA are, according to TNT, that apart from it being a “sales argument” for customers with attractive products, it also helps TNT to keep losses to an absolute minimum, at the same time as all TNT’s employees have a qualitative approach to security. In addition, membership has had the effect that cooperation with authorities has been facilitated. TNT has also been certified in respect of security in the Swedish Customs’ Stairway programme.

After TNT became a member only small details have been changed in TAPA’s programme approximately every second year, but none of these changes has made it necessary for TNT to make major investments or changes to its processes.

Prior to joining TAPA, TNT was at a very low level where thefts were concerned, and these have definitely not increased after membership. What the entire sector can see is that, when terminals are made secure, the criminal focus moves to transports between terminals, and therefore TNT is now considering accreditation under TAPA’s TSR (Truck Security Requirement) standard.

---

86 [www.tnt.com](http://www.tnt.com)
87 Questionnaire, Bengt Tufvesson, TNT, (2007).
PART C: ANALYSIS
Different perspectives on the security initiatives

One of the questions posed initially in this report concerned costs arising as a consequence of the security programmes and the possibility of calculating benefits that can be gained from the programmes. The National Board of Trade has not made its own study of costs. In this report the Board has chosen to present a review of the literature which takes up studies of both costs incurred by business and costs incurred by society in general. In this review we discuss how the increases in costs resulting from the initiatives are distributed between the parties involved. One central question is whether these costs affect competition between different regions. In the report the National Board of Trade also presents its own theoretical analysis of the importance of price elasticity for transports, which makes it easier to identify those parties in the supply chain that have to bear the largest proportion of the costs that arise as a consequence of the security initiatives.

In order to make an in-depth study of the ways in which the security programmes function, a model is needed which shows how the programmes have been constructed. Initially, a tentative division of the security initiatives was presented, based on the originator and focus of the initiative. Below we supplement and discuss the table presented in section 2.3 above.

In the study of literature on which this report is based, only a few systematic approaches have been found that attempt to classify and analyse the security initiatives. One of the most comprehensive attempts to systematize the certification programmes between customs authorities and the business associations’ own security programmes (TAPA, BASC), has been made by the Cross Border Research Association, an independent research organisation linked to the University of Technology in Lausanne (École Polytechnique Fédérale de Lausanne) and the School of Economics in Lausanne (HEC Lausanne). Their model and comparative study of the programmes are presented briefly below. With our point of departure in the comparison made in the Cross Border study, we will comment on the ways in which the programmes have developed and discuss the possibilities available for trade facilitation that can be drawn from the study. In addition, a couple of alternative approaches are discussed.

The importance of trade with the USA and the effects the American initiatives have had on the entire development of security programmes has been described and discussed in the sections above. During the period 2008 to 2013, the EU will further develop both customs operations and security systems. The way in which the systems in the USA and the EU are designed and the extent to which information can be transferred between them is of great importance for global trade. It seems possible that if the EU and USA can produce a system in which they accept each other’s structures, risk assessments, and even the exercise of powers by each other’s customs authorities, there are considerable benefits to be gained, not merely in coordination between these two major trade blocs, but also in the possibility that the systems will be copied and that other countries will adopt them. This would lead to considerable trade facilitation. Therefore, in a special section, comparisons are presented, first between C-TPAT in the USA and the AEO programme in the EU, and then between the advance notification regulations in the USA and the EU. The WCO’s SAFE framework is used as a common frame of reference. In this connection the aim is also to find where the systems overlap and to identify possibilities for trade facilitation and coordination.

In an OECD report a risk analysis model is presented which is applied to the risk of a terrorist group using the supply chain to deliver weapons of mass destruction. A brief summary of the content of the report is presented.

All in all, these analyses are intended to provide a framework for an analysis of the contents of the security programmes, for the presentation of a more detailed comparison between the EU’s and USA’s systems against the background of SAFE, and for a description of the costs and the threats which the programmes have been developed to meet.
9 What effects do the security initiatives have on trade?

Important questions in the literature on intensified security requirements in international trade concern the ways in which they affect trade, and the ways in which the security initiatives should be formulated to enable sufficient incentives for participation to be offered to the parties involved in the international supply chain. To facilitate the analysis of initiatives for security and facilitating trade, this chapter begins with a discussion of the economic effects of international terrorism. This makes an in-depth discussion of existing security needs possible. Then, by describing the economic mechanisms that lie behind the security measures in the international supply chain, any possible needs of a coordinated strategy between different parties involved, both companies and countries, can be described.

Thereafter, the discussion takes up requirements for making initiatives for security and trade facilitation financially effective and efficient from the security perspective. The costs of the security initiatives and trade facilitation provided by the initiatives are weighed up under this heading.

Incentives for companies to participate in security initiatives can have both a positive and negative character since they are partly based on threats against security and partly on possible benefits. Benefits related to enhanced security are often difficult to quantify and therefore such benefits will be treated in a qualitative way. The costs arising from stricter requirements are firstly presented at the general level, where the different types of costs are presented, as well as consequences for the international economy. The National Board of Trade’s analysis of the distribution of costs between the different parties involved is presented here in an attempt to identify the parties that have to bear the largest proportion of the costs. The analysis is based on standard economic theory.

Finally, analyses are presented of the different ways in which increases in transport costs, which can arise from the new initiatives, affect different types of products and different parts of the world. The focus of this discussion lies on whether or not developing countries in particular are negatively affected by increases in transport costs.

9.1 The effects of terrorism on the international economy

The attacks against the World Trade Center in New York and the Pentagon on September 11, 2001, had considerable economic effects, not only on the USA but also on large parts of the world. The attacks against the World Trade Center led to damage corresponding to USD 40 billion, the largest insurance amount in history. The flow of goods to and from the USA was stopped directly after the attacks and the country’s borders were closed for up to three days. At the global level these events created a great deal of uneasiness on the international finance markets. Companies in the international trade and logistics sectors were not merely affected by a reduction in demand, but also by costs related to intensified security requirements.

One sector that was affected particularly severely was air traffic. Demand, mainly for vacation flights, collapsed in the short term, and it took time to restore confidence in air transport as a means of transport. Moreover, the air companies were affected by a deterioration in their insurance terms. After the attacks the insurance companies both reduced insurance cover and increased premiums considerably.

Greater demands in respect of security increased the costs of companies working in the logistics and trade sectors. Longer times for customs clearance of goods had an additionally severe effect on those companies that are largely dependent on just-in-time deliveries, for example

companies in the automobile industry. Transport times were not just longer, they were also more unpredictable. This made production planning difficult for many companies working in international trade. On account of different proportions between the insurance costs of the goods and their value, differences in available modes of transport and the different roles of the goods in production processes, the transaction costs involved affected different sectors differently (see section on the costs of security).

At the local or regional level terrorism can have the effect that companies move their operations to safer areas. In addition, investments are affected, which affects the possibility of achieving economic growth. In New York these negative effects were slight since the city had an economy which promoted growth. However, other countries have not been as fortunate. The fate of Yemen is an example of how terrorism and a lack of security can have severe negative effects on growth. The attacks against an American destroyer, USS Cole, in Aden in the year 2000 and against the French oil tanker Limburg outside the coast of Yemen in 2002 have led to a serious deterioration in the country’s exports, and foreign investors who had previously planned to invest capital in the country have, in principle, abandoned the country. In this case terrorism has changed trade routes in an entire region. Other examples are the Egyptian tourist industry, which was severely affected after 63 Japanese tourists were shot to death in Luxor in 1997, and Pakistan, whose economy is severely affected by recurrent acts of terrorism.

In general it can be said that the costs related to a potential terrorist attack are very high and, even if it is difficult to assess the risks of an attack, this constitutes a strong incentive to make efforts to secure the international supply chain against possible attacks in the future.

9.2 Security as a collective good

Global security is a complex issue since it depends on the involvement of a large number of parties at different levels. However, it is possible to discuss security using its underlying economic mechanisms as the point of departure. In order to minimise the negative economic effects of terrorism directed towards the supply chain, investments can be necessary in measures to enhance security. These investments must be financed in one way or another. One problem with security from the financing point of view is that it has strong characteristics of a public good. Dulbecco and Laporte (200) describe the characteristics of security as a global public good. Primarily it generates externalities that benefit everyone; national and international as well as public and private parties. Moreover, global security requires contributions from all countries and from the different parties involved in the supply chain in order to function optimally. Security depends namely, according to the authors, on its weakest link, i.e. the lowest national contribution to global security. The supply of security requires a basic activity (mechanisms designed to develop a positive externality) and a complementary activity (measures that permit a country to make full use of the advantages derived through the development of an externality). This tempts parties involved to behave as free riders, to attempt to enjoy the advantages created by the investments of others without contributing themselves to security. One example of this is airports whose security

---

93 According to the Rosen-Roback model for regional equilibrium, threats of terrorism have effects on the labour and property markets in the area affected. Threats of terrorism are experienced by the population as a decline in their prosperity and, in order to persuade people to stay in the relatively unsafe area, higher wages and lower rents are necessary. The value of property declines at the same time as company profits come under pressure, which increases their willingness to move.
94 Bram, Haughwout and Orr (2002) applied the Rosen-Roback model to New York after the attacks against the World Trade Center, but found that these effects were small, largely due to the city’s industrial structure and working environment which promoted economic growth.
95 In economics, the concept “externality” is used for costs (negative externality) or benefits (positive externality) that arise for parties that do not participate in transactions or other economic activities.
depends to a certain extent on controls performed at other airports. Finally, global security is a
direct result of international agreements, which means that it is dependent on the efforts of a large
number of countries and it requires international coordination for its existence.

Dulbecco and Laporte (2003) point out that, from a game-theory perspective, lack of confidence
between the parties involved leads to a situation in which the most rational strategy is to transfer
the responsibility for investments to others so that one can share the enhanced security at no
cost. Globally this leads to suboptimal levels of investments in security. It can be very difficult to
tackle this problem at the individual level. 96 There is namely a risk that shortfalls in investments
in security can be the best strategy for each individual party concerned. 97 Furthermore, it is
in the nature of terrorism to adapt to the security measures of potential victims. When an
individual tries to protect himself, terrorist organisations tend to move their resources to other
targets. Lakdawalla and Zanjani 98 point out that the threat of terrorism thus generates negative
externalities since it leads to ineffective investments in private security. The combined effect of
the discussions in the two studies mentioned above, namely lack of confidence and the desire to
protect oneself, can be that investments in security that only protect the individual making the
investment are exaggerated, while investments in global security are inadequate. At the aggregate
level this can lead to a situation in which countries choose a strong national security strategy
at the expense of international coordination. This leads to the risk that unnecessary costs are
incurred since a coordinated security strategy would facilitate the harmonisation of routines and
avoid duplicating them.

The logical conclusion that can be drawn from the problems originating from the collective nature
of security is that coordination between the parties involved is necessary to achieve effectiveness.
This can take place in different ways and between different types of parties but, in general, it
constitutes a strong argument for a type of security initiative in which all parties involved in the
international supply chain are given sufficiently strong incentives to contribute to the global public
good, i.e. security. Dulbecco and Laporte (2003) point out that the WCO is the international
institution that can best coordinate financing and facilitate the creation of global security.

There is a risk that shortcomings in international coordination lead to an ineffective global system which
has a distorting effect on trade. There is thus also a risk that the goals of the security measures are not
fulfilled while their costs increase and are distributed to regions or parties that should not bear them.

9.3 How should effective security measures be designed?

One central issue when discussing the formulation of a security initiative is the way in which
security measures affect trade flows. Another issue is whether security can best be enhanced with
the aid of preventive measures or more inspections.

9.3.1 Security and trade facilitation

Many studies demonstrate that when traditional trade barriers such as customs and quotas
disappear, new trade barriers such as complicated trade procedures assume greater importance.
An often quoted OECD study estimates that the transaction cost of inefficient trade procedures
amounts to between 1 and 15 per cent of a product's value 99. The higher figure is more often the
case in developing countries where it is complicated and costly in terms of both time and money
to fulfil the requirements laid down for the import and export of goods.

96 Individual level in this context refers to both companies and countries.
97 If there is no coordination, each party's individual strategy depends on how the other parties are expected to
act. In some cases a situation may arise in which an underinvestment in security is the best strategy since all other
choices would result in a loss. In game theory this is referred to as the "Nash equilibrium".
98 Lakdawalla and Zanjani (2002).
This means that there are large potential gains to be made by facilitating trade procedures and thereby reducing transaction costs for international trade. Even for the countries that comparatively have the most efficient trade procedures – such as parts of Europe, Asia and North America – there is a great potential for trade facilitation, primarily by harmonising procedures between countries and taking advantage of IT solutions. UNCTAD (2001) studied the effect of measures for trade facilitation - such as the development of e-trade - and it was estimated that measures for trade facilitation would also generate a 3.3 per cent increase in APEC’s trade in goods.\textsuperscript{100}

When a study is made of the effects of the security initiatives on international trade, it is of interest to ascertain whether the increase in the number of security initiatives prevents the benefits of trade facilitation from being realised. Another question is the extent to which countries take a step backwards from trade facilitation they have implemented by giving the companies an increasingly complex set of regulations to comply with and by customs authorities increasing their controls.

Dulbecco and Laporte (2003) are of the opinion that even if security in the supply chain can be perceived \textit{a priori} as incompatible with the goal of facilitating and promoting the international trade in goods, this view does not stand up to closer analysis. The basic idea behind logistical activities is that the various stages can be divided up and implemented at different geographical locations. According to the authors, work on security corresponds well with this concept. Security as a global public good is also closely associated with the expansion and flow of international trade. Security and trade facilitation thus reinforce each other.\textsuperscript{101} If a certified operator benefits from trade facilitation, the result can be, at the individual level, greater efficiency in the logistical process through a reduction in costs for administration and controls, improvements in the flow of goods etc. At the global level trade can be positively affected. The authors are of the opinion that increased security leads to trade facilitation which, in turn, increases trade.

**9.3.2 Preventive measures or inspections**

Two types of fundamental approaches lie behind the security initiatives described in this study. One is creating greater security by increasing the number of inspections of containers and other consignments, and refining routines and instruments for these inspections. The point of departure of the other approach is that security is created by the analysis and management of risks and threats. With the exception of the USA's rule on 100 per cent scanning of containers, all the initiatives presented in this study have features of both these approaches. On the other hand, there are differences in the initiatives in respect of the approach which predominates.

Lee and Whang (2003) are of the opinion that preventive security measures are always to be preferred to inspections and point out experience gained from the quality assurance processes of companies as well as production models such as the so-called Toyota and Poka-Yoke systems for production, which are based on flexible processes and just-in-time deliveries. By introducing routines that permit immediate identification and remedy of deviations and shortcomings in production, these shortcomings can be avoided in the future. Losses are minimised at the same time as the production chain is made adaptable to changes. In this way quality can be enhanced without cost increases. In the opinion of Lee and Whang this can be transferred to security in the supply chain. Instead of investing in more inspections at the final destination of a transport, procedures that prevent a container from being manipulated before and during transport should be designed and introduced. They mention CSI and C-TPAT as examples of initiatives that follow this concept, in that both have been designed to secure the supply chain closer to its origin.

The idea behind the USA's requirement for 100 per cent scanning, which will come into effect in 2012, has received strong criticism from, among others, the WCO which feels that there is misunderstanding in respect of the relationship between security and the proportion of containers

\textsuperscript{100} Wilson et al. (2004), p. 193.
\textsuperscript{101} Dulbecco and Laporte (2003), p. 4.
inspected. Instead of inspecting everything, there should be an ambition to have an enhanced and more clearly focused risk analysis. The EU Commissioner for Taxation and Customs Union, László Kovács, has also expressed concern that the initiative affects the balance between security requirements and trade facilitation.\footnote{European Commission, Midday Express, 2 August 2007.}

It is difficult to determine whether security initiatives function as trade barriers or whether in actual fact they facilitate trade flows. In order to make an analysis of this type, the question should be made more complex: among other things the time aspect should be taken into consideration. Some initiatives can lead to benefits and trade facilitation in the long term, but function as a trade barrier in the short term. In order to avoid a situation in which the initiatives function as barriers, the costs should be carefully weighed against the possible benefits that might arise from the intensification of security requirements. The idea of scanning all goods goes against the idea of efficiency and trade facilitation, and there is a risk that it will act as a trade barrier.

\section*{9.4 Analysis of the benefits and costs of the security initiatives}

What will be the result of the increased investments in security in the supply chain for the various parties involved? In general it can be said that making a comparative analysis of costs and benefits is extremely difficult. In part it is the benefits that are particularly difficult to calculate in monetary terms since it is almost impossible to calculate the probability of terrorist attacks. Therefore, the costs and benefits are presented separately and the National Board of Trade refrains from making a cost-benefit analysis.

\subsection*{9.4.1 Benefits of the security programmes}

As opposed to the costs incurred as a result of stricter security requirements, which are often possible to calculate quantitatively, it is difficult to measure the direct benefits of enhanced security apart from a reduction in losses due to theft. The problem lies in the actual nature of the benefits, since it is not possible to determine the costs that arise from a breach of security that never takes place. In this respect, Rice and Spayd (2005) point out the irony in the fact that it is only possible to calculate the benefits of a security measure when it has failed.\footnote{Rice and Spayd (2005), p. 7.} The search for benefits, or rather the savings generated by an incident not occurring, is made additionally difficult by the fact that companies are reluctant to disclose detailed information about their losses. There is a risk that information of this type may weaken companies, vis-à-vis both competitors and the general public, which can lead to losses for the companies. The companies also lack an incentive to share this information with insurance companies since they would adjust premiums to reflect the increase in losses.\footnote{Rice and Spayd (2005), p. 7.}

Cordes et al (2006) attack the problem by calculating willingness to pay by measuring actual preferences and choices made by individuals and companies in different markets. Changes in consumer surpluses are given prominence as the best method of calculating willingness to pay. Put simply, a consumer surplus can be defined as the number of units of a certain product which a consumer had been willing to pay more for, but has obtained at a lower equilibrium price. The costs of security measures increase the price of a product which reduces the consumer surplus, partly since each unit now costs more and partly since the consumer consumes fewer units of the product.\footnote{See figure 9.1.} The authors provide three examples of ways in which the consumer surplus can be estimated: an increase in costs on account of travel time; an increase in costs due to delays in the transport of goods and services; and an increase in costs due to a loss of amenities.\footnote{Cordes et al. (2006), p. 16.} A further problem presented in relation to the analysis of costs and benefits of a security initiative is the issue of discounting. This can be explained in brief as follows: a certain sum spent in the form of

\footnotesize
\begin{itemize}
  \item European Commission, Midday Express, 2 August 2007.
  \item Rice and Spayd (2005), p. 7.
  \item Rice and Spayd (2005), p. 7.
  \item See figure 9.1.
  \item Cordes et al. (2006), p. 16.
\end{itemize}
costs or generated as a profit has a higher value at the present time than in the future. The authors write about the social discount rate, a type of interest rate as an indicator of the extent to which society discounts future costs and profits. A base discount rate of seven per cent is mentioned for investments in measures made by the United States Department of Homeland Security.\(^{107}\)

The result of this study was that the possible direct benefits of preventing a terrorist attack against San Francisco and Oakland, which was based on a model constructed on the basis of the attacks in New York, would amount to approximately USD 12.2 billion. The estimated cost of raising the level of security in these cities was USD 9.6 million. The total costs of increased waiting time at airports and on highways resulting from the new security measures was estimated at USD 14.2 million. In other words the total sum of the costs would be USD 23.8 million. The analysis shows that the risk of a terrorist attack must be at least two-ninths of one per cent (0.0019) to make the investments in enhanced security correspond to the benefits.\(^{108}\)

At the company level Rice and Spayd (2005) choose to specify the direct and indirect beneficial side-effects of security on the basis of different groups of security measures, which are included in many of the initiatives included in this report. The main spin-off effect is said to be the possibilities available to companies to continue operations during periods of disruptive incidents. This benefit is achieved since the probability of the supply chain being broken diminishes, and that production can be resumed more rapidly in cases when it is broken. Depending on the type of measures introduced, the companies can, according to Rice and Spayd, also enjoy further benefits with investments to secure the supply chain.

\subsection*{9.4.2 Costs of security}

Even if there are arguments that heightened security pays for itself in the long term, it implies costs in both the short and long term. A central theme in the discussion on stricter requirements for security is the extent to which the parties involved in international trade are affected by an increase in transaction costs. Longer times for customs clearance and handling goods, as well as higher insurance premiums, lead to costs that can have negative effects on efficiency in trade. In order to be able to calculate these costs in a simple way, they are often compared with a customs tariff on the value of a product. Walkenhorst and Dihel estimated these costs at up to three per cent of the value of a product in March 2002, but reduced this estimate to up to one per cent in 2006. The lower estimate corresponds to costs of up to USD 75 billion per year.\(^{109}\)

In the discussion on increases in transaction costs the time aspect cannot be overemphasised. There is a risk that intensified security requirements for customs clearance and demands in respect of advance notification will slow down the supply chain. This will force costs up and thus have a negative effect on the profitability of the parties involved. Longer transport times at sea mean both an increase in storage costs and depreciation of the value of the product. However, it is not only the risk that the length of transport times is increased by intensified security requirements in the supply chain; transport times can also vary more. This can result in serious problems, primarily for those companies whose production is dependent on just-in-time deliveries. There is a risk that a delay in deliveries of a key component in a company’s production chain will stop production of the product in question entirely. Variations in transport times can thereby give companies an incentive to abandon their just-in-time production activities and increase their stocks, with a resultant increase in costs.

Hummels (2001) has calculated costs related to increases in transport times and arrived at the conclusion that each day a product is being transported at sea is equivalent to a tariff of 0.8 per cent

\(^{107}\) Cordes et al. (2006), p. 29. United States Department of Homeland Security is the USA’s federal department responsible for protecting the country against terrorist attacks and for taking measures in cases of natural disasters.

\(^{108}\) Cordes et al. (2006), p. 82.

on the value of the product.\textsuperscript{110} The average duration of maritime transport for goods exported to the USA is 20 days which corresponds to a tariff of 16 per cent. This can be compared to air freight which, in 1998, normally corresponded to a premium of 25 per cent of the value of a product.\textsuperscript{111} The probability that air freight is preferred to sea freight is a function of the difference between the charges made by sea and air transporters, and the number of days required for each mode of transport. For an average product this has the result that, if the duration of transport by sea exceeds 31 days, it is more profitable to change to air freight, which in general takes less than 24 hours regardless of where the product is shipped from. Air freight's proportion of total transports has increased dramatically since the 1950s, primarily due to the fact that the costs of air freight have decreased considerably, at the same time as the real prices of sea transport have remained constant or have risen.\textsuperscript{112} This trend can be reinforced by longer transport times which can also exacerbate climate problems.\textsuperscript{113} Air transport is more often chosen by manufacturing companies, particularly companies whose products have a high rate of depreciation, for example newspapers and PCs, as well as in sectors in which demand is difficult to predict, for examples the fashion and toy industries.\textsuperscript{114}

Hummels (2001) has studied the effect of increases in transport times by looking at the relationship between transport time and exports, and found that for every day a transport from a country is extended, the probability that the USA imports from that country diminishes by 1-1.5 per cent. For many countries their geographical location, terrain and shortcomings in infrastructure function as effective trade barriers. At the same time, Limão and Veneables (1999) point out that countries with common land borders tend to experience lower transport costs compared to other countries, not just on account of shorter distances but also through a more highly integrated transport network, more harmonised customs routines and greater possibilities of using so-called backhauling, i.e. using the mode of transport in question in both directions.\textsuperscript{115} One possible result of increases in transport costs could therefore be that trade between neighbouring countries increases at the expense of trade over longer routes. From the trade theory perspective this represents an economic loss since comparative advantages are lost when an increase in transport costs leads to suboptimal selection of trade partners.

By comparing transport costs\textsuperscript{116} and trade volumes, Limão and Veneables (1999) deduce the price elasticity of trade flows in relation to transport costs.\textsuperscript{117} This elasticity proved to be high, approximately -2.5. This means that a one per cent increase in transport costs reduces the volume of trade by 2.5 per cent. Limão and Veneables also say that halving transport costs would lead to a fivefold increase in the volume of trade.\textsuperscript{118} Increases in transport costs reduce trade flows, particularly between countries at a great distance from each other.

\textsuperscript{110} This cost varies with the nature of the goods. Hummels arrives at the conclusion that costs related to transport times increase if the value of the goods is relatively high, since depreciation is expressed relative to the value of the products. Office equipment had the highest value: a tariff corresponding to 2.2 per cent per day. This is an average value for trade with the USA and there is reason to believe that the value is higher for countries where the cost of transport already represents a large proportion of the value of the goods.

\textsuperscript{111} Cordes et al. (2006), p. 2.

\textsuperscript{112} Hummels points out here that the price of air transport has decreased in real terms by almost six per cent since the Second World War.

\textsuperscript{113} The growing proportion of air freight as a part of all transport has led to concern where environmental issues are concerned. An England-based environmental organisation, Soil Association, points out that the emission of carbon dioxide for each kilo of a transported product is 177 times higher for air freight than for sea freight.

\textsuperscript{114} Hummels (2001), p. 3.

\textsuperscript{115} Limão and Veneables (1999), p. 3.

\textsuperscript{116} As an indicator of transport costs Limão and Veneables use Cif (cost, insurance, freight)/Fob (free on board). This is then compared with trade volumes to produce the degree of elasticity.

\textsuperscript{117} Price elasticity for trade in respect of transport costs is an indicator of the degree to which trade is changed by a change in costs. If the price, or the costs, increase by one per cent, and the volume trade diminishes for this reason by one per cent, the elasticity is equal to one.

\textsuperscript{118} It should be pointed out that since elasticity in general diminishes with quantity, this assertion is far from logically obvious.
9.4.3 Who bears the costs of enhanced security?

Are there winners and losers among the parties involved in the supply chain, and if so, who are they? This section is based on an economic analysis made by the National Board of Trade with the objectives of shedding light on the mechanisms that lie behind the distribution of security-related costs, and of attempting to identify the parties that are most negatively affected by these costs.

In common with estimates of willingness to pay, this issue is strongly linked to consumer and producer surpluses\(^\text{119}\) and thus to supply and demand elasticity. When a cost is introduced in the production and distribution of a product, in the form of a fee or a tax, the producer usually tries to pass on this cost to the consumer. This can seem to be easy – the producers simply raise the price the consumers have to pay. The problem is that, apart from in exceptional cases, this leads to a reduction in the quantity sold. Normally, when supply and demand elasticity, i.e. the producers’ and consumers’ price sensitivity in respect of quantity, is equally great, they share the costs of the fee or the tax. In figure 9.1 these costs correspond to the difference between \(p_1\) and \(p_2\). The area AB corresponds to the reduction in the consumer surplus, which consists of the price increase of each consumed unit of product (A), as well as a pure welfare loss due to the reduction of the consumption of product (B). CD corresponds to the reduction of the producer surplus, which consists of the reduction in payment for the product or service (C), as well as the pure welfare loss due to the reduction in consumption of product (D). BD is the so-called deadweight loss that arises from the new security-related cost.

![Figure 9.1 A security-related cost (ABCD) is distributed equally between consumers and producers](image)

Figure 9.1 illustrates that as long as supply and demand elasticity are equally great (supply and demand curves have the same angle but opposite signs), the producer and the consumer share the cost equally between themselves. On the other hand, if the elasticity of supply or demand is different, the cost will be distributed asymmetrically. One common factor for supply and demand is that higher elasticity for one of them relative to the other has the effect that costs are transferred to the other. On the other hand, low relative elasticity has the effect that the producer or the consumer must bear the largest proportion of the cost.

\(^{119}\) Put simply the producer surplus is the quantity of goods that are sold at the equilibrium price, that the producer had been willing to sell at a lower price.
With this discussion as the point of departure an analysis can be made of the ways in which security-related costs are distributed among consumers and producers in maritime and air transport.

Maritime transport of containers is a sector that in recent years has been characterised by overcapacity. A surplus of container ships compared to the number of containers that needs to be transported has had the effect that the shipping companies’ customers can benefit from competition among the shipping companies by putting pressure on prices. The demand for the services of the shipping companies thus becomes more elastic, which is illustrated schematically in figure 9.2.

![Figure 9.2](image)

**Figure 9.2** Overcapacity in marine transport leads to high demand elasticity, represented in the figure by the flat angle of the demand curve. This high elasticity has the effect that the producers, in this case the shipping companies, have to bear the largest proportion of the new costs.

Despite the fact that the prices increase somewhat for the shipping companies’ customers, mainly importers and exporters, it can be maintained that they are the relative winners and the shipping companies the relative losers due to increases in the costs of security.

At the time of the attacks against the USA on September 11, 2001, the maritime and air transport sectors were characterised by overcapacity. This had the effect companies in these sectors were unable to pass on the costs that they incurred from the new security requirements. Air passenger traffic was particularly severely affected since a collapse in demand, particularly for vacation flights, had the consequence that the price of air tickets even fell in the short term.\(^\text{121}\)

---

\(^{120}\) Heymann (2006) p. 4.

Air passenger traffic was severely affected by the attacks on September 11, 2001. A collapse in demand combined with increases in the costs of security, had the effect that the number of journeys fell in two steps from \( q_0 \) to \( q_1 \) and from \( q_1 \) to \( q_2 \). Due to overcapacity at the airlines, high elasticity (represented in the figure by the demand curve's flat angle) had the consequence that the largest part of the increase in security costs was borne by the airlines. This means that prices fell after the attacks, from \( p_0 \) to \( p_2 \) despite the new costs of security. The model illustrates what happened in the short term. In the long term a new equilibrium price generally comes into being since the supply curve also shifts.

With the existing overcapacity in these sectors there is reason to believe that it will continue to be difficult for the companies to pass on the costs to their customers. Heymann (2006) has predicted that the available capacity of container ships will increase by approximately 50 per cent between 2006 and 2008. With an estimated growth in container handling of nine per cent up to the year 2015 there is a considerable risk that a number of years will have to pass before the supply of container ships is in balance with demand for container transport.

9.4.4 The consequences of security for competition

How is competition affected by these costs? Even if the increase in transaction costs is a global phenomenon, certain parties, sectors and geographical regions are more seriously affected than others. According to Walkenhorst and Dihel (2006), an increase in security not only means that importing and exporting countries are affected, it also causes a change in trade flows and substitution of goods. The EU Commission has expressed concern about the fact that the USA, through CSI, is changing trade flows, since trade from ports which are not CSI certified is being transferred, for example to Rotterdam. This, in the opinion of the Commission, is against the EU’s competition rules.

Different products are affected differently by the introduction of new security requirements. Walkenhorst and Dihel (2002) deduce this from the differing proportions between transport

---

and insurance costs and the value of the goods, differences in access to different modes of transport, and the different roles of the goods in production. Trade in raw materials that have a large weight and volume in relation to their value, such as fertilisers, coal and certain fruit and vegetables, tend to be affected more negatively by increases in transaction costs.\textsuperscript{125} Longer transport times can also lead to a situation in which producers of agricultural perishable goods choose not to ship their produce abroad.\textsuperscript{126} One example is the USA’s Bioterrorism Act of 2002. According to this act, advance notification is required for the transport of foodstuffs. This affects in particular certain agricultural products with a short life cycle. It has been pointed out that there is a risk that this act will lead to a situation in which importers in other countries choose to buy these goods from other places.\textsuperscript{127}

There is a risk that security-related costs not only affect different sectors asymmetrically; differences in the rules can also lead to the costs being distorted in sectors in different parts of the world. An important question for parties involved in both air and maritime transport is: who is financing the new costs: the state or the sector? In December 2002, the EU Commission introduced common rules for civil air safety in the member states.\textsuperscript{128} The ways in which these rules were implemented differs between the different member states. The centralised model means that the responsibility for security activities mainly rests with each state via its aviation authorities, ministries of transport, police authorities or the like. Eleven European countries have this model: Finland, Iceland, Italy, Luxembourg, Norway, Portugal, Switzerland, Spain, Sweden, Germany and Austria. The decentralised model means that security activities are mainly performed by airports under the supervision of the relevant authority. Belgium, France, Greece, Ireland, the Netherlands and Great Britain follow this model.

In general, the centralised model means that a relatively large proportion of security-related costs can tend to end up with the state and a smaller proportion with the airports and airlines. The USA has had a highly centralised model for financing and divisions of responsibilities where air security is concerned after the federal government, via the Transportation Security Administration (TSA), took over the responsibility for the main security measures in November 2001. Voices have been raised among European airlines and airports that competition with their American counterparts is not fair since the latter receive considerable federal support, and have therefore demanded that, in each European country, the state should bear a greater proportion of the new costs.\textsuperscript{129}

Walkenhorst and Dihel (2006) state that although North America would suffer considerable welfare losses from increases in transaction costs, other regions which are much more dependent on international trade, such as Asia or North Africa and the Middle East, would be more seriously affected in relative terms. Furthermore, they feel that it is agricultural products and food, as well as textiles and leather products, which would probably be the most severely affected since these sectors are politically sensitive and often characterised by protectionism.

Dulbecco and Laporte (2003) state that ports are the most sensitive link in the supply chain since they handle a large part of the international trade and are a meeting place for a large number of parties in the private and public sector. Moreover, they claim that the expenditure on security is without doubt largest at the ports.\textsuperscript{130} They point out that the ports themselves finance port security measures and that financing directly from the private sector has three disadvantages: it leads to an inadequate level of global security due to its collective character (see section on security as a global public good); it leads to distortion of competition between operators and countries; and it leads to the risk that requirements for certification will force out operators from countries that have not made so much progress in the field of security.

\textsuperscript{125} Walkenhorst and Dihel (2002), p. 13.
\textsuperscript{127} Wilson et al. (2004), p. 183.
\textsuperscript{129} Irish Aviation Society/Aviasolutions (2002), p. 4.
\textsuperscript{130} Dulbecco and Laporte (2003), p. 7.
In order to minimise these problems the authors are of the opinion that the WCO is the global institution that best can coordinate financing and facilitate the creation of global security.11 This is a reasonable conclusion since the WCO’s SAFE framework is the most ambitious initiative at the global level, partly because it develops cooperation between customs authorities in different countries and between customs authorities and companies, and partly since it includes all modes of transport. Moreover, SAFE has the clearly expressed ambition to introduce trade facilitation at the same time as security is strengthened, which can minimise the risk that stricter security requirements function as trade barriers.

9.5 How are developing countries affected?

Another important point that should be taken up where security initiatives are concerned is the way in which they affect countries with different welfare levels. One central issue is how the economies of developing countries are affected, and whether these countries are particularly negatively affected by stricter security requirements.

Many developing countries already have a difficult trade situation. Difficult terrain, shortcomings in infrastructure and considerable distances from trade partners are serious trade barriers for many developing countries and therefore transport costs constitute a larger proportion of the value of goods in these countries compared to richer countries. Wilson et al. (2004) state that the transport costs of developing countries are generally two to four times as high as in rich countries.12 Where transport times at sea are concerned, Hummels (2001) lists three interesting characteristics of developing countries.13 Firstly, the average developing country is farther from destination markets than richer countries, which means longer transport times. Secondly, the volume of goods is smaller, which has the effect that ships must stop in more ports in order to fill up. Thirdly, the frequency of transport is much lower than for rich countries. In this connection, Hummels (2001) points out that ships from Japan arrive at an average port in the USA every day, while ships from Africa arrive every fifteenth day.14 If a delivery is ready for shipment on March 1, for example, but the next ship does not depart until two weeks later, the effective transport time is the time onboard plus this waiting time. To return to Hummels’ calculation, i.e. that each day’s delay in transportation corresponds to a tariff of 0.8 per cent, this can be a major problem for these countries’ exports.

According to Amjadi and Yeats15, transport costs to other countries amounted to 15 per cent of African exports in 1990. This is much higher than for non-African countries. Furthermore, Wilson et al. (2004) point out that developing countries are particularly sensitive to cost increases arising from threats to security, due to severe budget limitations, their great dependence on foreign trade and investments, and their obsolete infrastructure. This is further exacerbated by a number of problems that are characteristic for many developing countries:

- Frequent reloading of goods,
- Overloading and bottlenecks in ports, which affects throughput times for feeder ships,
- Complicated customs procedures,
- Complex and non-transparent administrative requirements, which often apply to documentation,
- Limited use of computerisation which leads to high costs from information management,
- Uncertainty regarding the extent to which legal trade documents such as sea freight notes and letters of credit are valid.

11 Dulbecco and Laporte (2003), p. 34.
Wilson et al. are of the opinion that there is a risk that these problems, in combination with difficulties in meeting the requirements for certification, principally in respect of customs clearance, will exclude the exports of developing countries from global trade.

Dulbecco and Laporte (200) feel that developing countries are systematically punished due to the fact that they are not at the same level in respect of security certification. At the same time they do not necessarily constitute a high risk. They therefore advocate a differentiation of costs and routines for risk assessment with the effect that those who constitute the greatest risk should bear the highest costs. Even if it can be maintained that this would create incentives for high risk operators to improve their routines and their infrastructure to enhance security, it would probably have a very serious effect on trade in countries such as Pakistan, which has been affected by a number of terrorist attacks in recent years.

As more and more countries introduce certification programmes for security in the supply chain there is a risk that countries that lack resources and have inefficient systems for the exchange of information and security controls will not share the benefits promised by these programmes and even experience a deterioration in their prospects of participating in international trade. There appear to be strong reasons for paying particular attention to the situation of developing countries. The ambition of facilitating the integration of developing countries into the trade system is best achieved by giving support to those countries that want to implement measures to fulfil security initiatives. The WCO Columbus Programme has the aim of giving this type of support to countries that implement WCO’s SAFE framework.

9.6 Summary and conclusions

It is quite clear that international terrorism has considerable negative effects on the international economy and that the supply chain is sensitive to external threats. The attacks against the USA on September 11, 2001, have led to a deterioration in the business climate for many companies in the form of increases in insurance premiums and costs related to intensified security requirements. Airlines and shipping companies were two sectors that were severely affected by this development. Furthermore, terrorism tends to affect the flows of trade and investments. This is clear in the cases of Yemen, Egypt and Pakistan. One central problem related to global security is that it is a global public good in that investments in global security measures imply a positive externality for all other parties. With a game theory perspective as the point of departure, this gives an incentive to parties to act as free riders, i.e. to benefit from the investments in global security made by others at the same time as they minimise their own investments. Meanwhile the threat of terrorism constitutes a negative externality which can lead to excessive investments in national security while investments in global security are neglected. In other words, global security is a direct result of the international policy. Dulbecco and Laporte (200) point out the WCO as the international organisation that can best coordinate financing and facilitate the creation of global security.

Terrorism is often used as the main reason for introducing new security initiatives. However, it is not only security that is in focus in these initiatives. Making trade and logistical chains efficient is another argument that is often used in discussions of the benefits of introducing new security requirements. This leads to the question of where the balance between the costs of security and trade facilitation lies. The National Board of Trade does not attempt to explain how this balance appears in the different security initiatives, but notes that there are considerable savings to be made by simplifying customs routines and making logistical chains more efficient, and that most of the initiatives presented in this report lead to both benefits and costs for the different parties involved in the supply chain.

The costs of transport resulting from intensified security requirements can prove to be considerable. Hummels (2001) points out, as mentioned above, that each day a product is
being transported at sea is equivalent to an average customs tariff of 0.8 per cent. The fact that international trade, with an elasticity of -2.5 per cent, shows a great degree of price sensitivity in respect of transport costs is evidence of the importance of minimising the costs of the increases in security requirements in the supply chain. To minimise these costs it is reasonable that the security initiatives should be based, as far as possible, on risk analyses and risk management, rather than on an increase in the number of inspections. Inspecting all containers can prove to be costly and involves the risk of unnecessarily slowing down international trade flows. Countries that are greatly dependent on trade and whose transport costs already constitute a large proportion of the value of goods are probably those that are most severely affected by extended transport times. Here the focus should lie on differences between different geographical regions.

Concern has been expressed about the risk that enhanced security can distort competition, both among the producers of different goods and between different geographical regions. High transport costs due to great distances to trade centres, difficult terrain, and shortcomings in infrastructure in many developing countries have placed these countries in focus in this discussion. Resources are required, both in the form of financing and know-how, to implement the security initiatives. In countries where capacity is already limited there is a risk that the intensified requirements for security in the supply chain will be a factor that reduces the possibilities available to them of participating in international trade. To reduce this risk, donor countries and international organisations have the responsibility to contribute support to these countries. One example of this is the WCO’s Columbus Programme which supports developing countries in their introduction of SAFE.

In sum, it is quite clear that both benefits and costs are distributed asymmetrically among the different parties involved in the supply chain. The economic analysis of the maritime and air transport sectors in this chapter indicates that as long as there is overcapacity in these sectors the companies will have difficulties in passing on security-related costs to the final customers.
10 Finding an analytical tool for the security initiatives

In section 2.3 of this report: *Introductory review of the security initiatives* some of the security initiatives are briefly presented and classified on the basis of whether they are governmental or non-governmental initiatives and whether they are voluntary or legally binding. In the more detailed presentation in Part B there is a discussion of the parties responsible for the initiatives and their focus. With the aid of the survey presented in Part B we can now supplement the analysis and classify all the initiatives. At the same time we extend the analysis by specifying what the driving forces behind the initiatives can be assumed to be. See table 10.1 below.

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Focus</th>
<th>Driving force</th>
<th>Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs authorities or other government authorities</td>
<td>Certification customs-companies</td>
<td>Greater efficiency</td>
<td>C-TPAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rapid recovery after incidents</td>
<td>FAST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AEO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>StairSec</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COMPACT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Frontline</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure Exports Scheme</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Golden List Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure Trade Partnership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AEO – WCO (BASC)</td>
</tr>
<tr>
<td>National or supranational bodies (EU, UN)</td>
<td>Information requirements</td>
<td>Basis for risk analyses</td>
<td>Advance notification EU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Advance notification USA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Advance notification WCO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Safe Port Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISPS code</td>
</tr>
<tr>
<td>National or supranational bodies (EU, UN)</td>
<td>Mandatory legal requirements for minimum levels of controls and protective measures</td>
<td>Minimum rules for security and safety Security controls</td>
<td>ISPS code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100% scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CSI</td>
</tr>
<tr>
<td>Private companies</td>
<td>Standards and Spreading information</td>
<td>Fewer thefts/ less smuggling</td>
<td>TAPA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BASC</td>
</tr>
<tr>
<td>Standardisation bodies</td>
<td>Implementation of certification programmes</td>
<td>Trade facilitation</td>
<td>ISO 28000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical uniformity</td>
<td>WCO- SAFE</td>
</tr>
</tbody>
</table>

Table 10.1 The security initiatives classified by initiator, focus and driving force.

It should be noted that certain initiatives cannot be classified exclusively in one category. This is naturally a problem for the classification in the table but it also provides a picture of the ways in which the programmes have developed over time. BASC is a clear example in which a company initiative to prevent smuggling has focused increasingly on security and is approaching C-TPAT in design and organisation. Most of the initiatives are also certification programmes. This is natural since so many states are members of the WCO and have approved the WCO’s SAFE framework. This means that in the near future we will perhaps see an explosive increase in certification programmes.
based on the WCO's definition of AEO. The challenge will be to harmonise these programmes so that it will not be necessary for companies to undergo the certification procedure in each individual country.

Where the customs authorities are concerned, there are rational driving forces behind the certification programmes. As world trade increases the customs authorities have greater incentives to rationalise operations to enable them to concentrate their efforts on goods that are considered to constitute a risk. One great advantage of allowing the companies to do much of the work of submitting information and performing security controls is that it is easier for the companies to identify the risks in their operations. At the same time it is important for the national economy of each state that trade can rapidly resume after an incident. In this connection the certification programmes are an important instrument. The certified companies will be able to be the first companies to restart their supply chains in a situation of this type.

Standardisation work is pursued by different international organisations whose activities have a different focus. The classical standardisation work is based on providing technical standards for equipment and working methods for the secure implementation of different initiatives. The WCO's guidelines for customs cooperation and cooperation between customs authorities and companies have another focus. They have the aim of facilitating trade and there is a common level of security at which customs authorities are able to share information with each other and benefit from each other's work.

### 10.1 Supply Chain Security Management

In section 2.4 a model was presented for the analysis of security programmes produced by the Cross Border Research Association in Lausanne. See figure 10.1. As we stated above, the researchers, Gutiérrez and Hintsa, are of the opinion that all security work can be classified into the following goals or categories:

- Facility Management
- Cargo Management
- Human Resources Management
- Information and Communication Management
- Business Network and Company Management Systems

![Figure 10.1 Supply Chain Security Management](image)

Figure 10.1 Supply Chain Security Management. Source: Cross Border Research Association/Gutiérrez and Hintsa (2006).

Gutiérrez and Hintsa are of the opinion that these components, in combination, build a system for Supply Chain Security Management. The classification can possibly be criticised for focusing too much on processes relating to the logistical chain and not so much on the freight of goods itself. In actual fact certain critics have expressed the opinion that all the security initiatives merely move the risks from one part of the system to another – often to the maritime transport of goods. However, the classification has great value since it appears to be comprehensive and makes possible a discussion on the content of the various certification programmes.

In a presentation made in 2006, Gutiérrez and Hintsa broke down the first five goals into activities and used them to make a comparison between nine different security programmes: PIP, BASC, TAPA, C-TPAT, Secure Export Partnership, StairSec, WCO, AEO (EU) and ISO.\textsuperscript{137}

To be able to analyse the certification programmes on the basis of the activities they include is an obvious advantage. A number of concrete measures are collected in each category. For example, the category Human Resources Management is broken down into five sub-categories:

- Employee hiring/exit process
- Personnel training
- Information dissemination
- Organisational roles and responsibilities
- Security culture development

Gutiérrez and Hintsa provide examples for each sub-category. Where the employee hiring/exit process is concerned, mention is made of background checks and interviews with employees who leave a company. See further table 10.2. This provides a relatively high degree of concretion even if the specification cannot claim to be completely exhaustive. Gutiérrez and Hintsa state that a relatively large number of the voluntary security measures are included in a large proportion of the various security initiatives in their study. The Swedish Customs claims that many of the stages that the Cross Border study states are lacking in StairSec are included in other parts of their Stairway programme. Since it is not possible to be certified in StairSec alone, there should be even greater correspondence between the programmes for this reason. The initiatives that Gutiérrez and Hintsa examined have been further developed since the study was published in June 2006. For example, it would appear the C-TPAT’s rules for the design of warehouses and loading premises have been developed so that they correspond well\textsuperscript{138} with the first category listed by Gutiérrez and Hintsa: Facility management – warehouse/terminal layout design, which, however, is not shown against C-TPAT in table 10.2. Without making a full review of the entire material it can thus be said that correspondence between the systems has rather increased than decreased over time.

The systematic approach is of great value and facilitates constructive comparisons. In this report the results will thus be used as a point of departure for a comparison between C-TPAT and the EU’s AEO system.

\textsuperscript{137} Gutiérrez and Hintsa (2006).
\textsuperscript{138} U.S. Customs and Border Protection, C-TPAT Importer Security Criteria (2005), www.cbp.gov
<table>
<thead>
<tr>
<th>Security Measure / Security Initiative</th>
<th>WFP</th>
<th>IASC</th>
<th>IFAD</th>
<th>GATT/WTO</th>
<th>HOS</th>
<th>PDO</th>
<th>ISO 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Facility management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Warehouse/terminal layout design (entry/exit controllability; clearly marked control areas; adequate product marking, sufficient light conditions etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Inventory management and control (adequate management of inventory information;use of product marking standards etc.)</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Facility protection (fences/locks; walls; minimization of exit and entry points etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Facility monitoring (24hr camera system, security guards, filming activities of loading containers, picking etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.5 Access/presence control processes and technologies (id / badges; smart cards; biometrics etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2. Cargo management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Prevention, detection and reporting of shipping process anomalies (routes and schedules continuous review; alerts management; detection and follow-up of averages and shortages etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Inspections during the shipping process (in points where liability changes, to packaging materials and vehicles before getting in contact with cargo, reporting of shortages averages etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 Exploitation of cargo inspection technical solutions (use of various scanners; nuclear/chemical/biological weapon sensors/detectors etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4 Exploitation of cargo tracking technical solutions (bar codes, RFID, satellite tracking, etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 Exploitation of cargo and vehicle anti-tampering technical solutions (use and control of high security seals; vehicle immobilisation devices, etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Human resource management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1 Employee hiring / exit process (background checks; interviews for leaving or fired employees etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.2 Personnel training process (continuous training on security issues; risk awareness etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.3 Information dissemination process (internal and external publication of the company security policies)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4 Organisational roles and responsibilities (establish security goals, assign security responsibilities to personnel, identify security required skills etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5 Security culture development (motivation and incentive programs targeting for cooperation and engagement with security issues)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Information management systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1 Quality information/data management (manage more complete and accurate shipment information, establish error-proof documentation processes, data integration etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2 Protection of business information/data management procedures and storing methods design to protect information from unauthorized access and usage)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.3 Records of shipping information for potential security audits (maintainsance of complete records of the custody of cargo, improved recordkeeping methods; quality control of records, errors correction etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4 Data exchange with Customs administrations (readiness to provide complete and on-time information as required; in particular compliance with Advance cargo information schemes etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.5 Use of International standards for data management (WCO Customs Data model, Unique Consignment Reference, digital signatures, digital certificates etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Business network &amp; Company management systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Company security management system (defined and documented security processes, defined and controlled security indicators, internal and external audits, etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2 Logistics system designed to reduce risks (evaluation of scenarios of natural risks, accidents, intentional human acts, terrorism etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3 Logistics system designed to guarantee quick event disaster/failure recovery (contingency plans, additional capacity, alerts management etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4 Business partners evaluation system (selection of low risk and high security compliant suppliers, clients and subcontractors)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5 Establishment of collaborative relationships with Customs administrations and other border agencies with control or security functions, procedures for the notification of anomalies or illegal activities. Consultation customs regulations and security matters.</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10.2 An overview of the elements that are included in the different security initiatives. Source: Cross Border Research Association/Gutiérrez and Hintsa (2006).
10.2 A comparison between C-TPAT, AEO and WCO

10.2.1 The major certification programmes – a step by step comparison

With the Cross Border study presented above as the point of departure, a comparison is made below between the certification programmes C-TPAT and the EU’s AEO system, and the WCO’s SAFE framework in respect of AEO. In order to make this comparison, the table produced by Gutiérrez and Hintsa has been studied first and updated where necessary.

Since C-TPAT has been developed after the publication of the Cross Border study and since the EU’s rules for its AEO programme have only been published in detail quite recently, it is necessary to update the table in order to make a fair comparison of the programmes. One of the cases where the programmes C-TPAT and AEO (EU) do not correspond in the study made by Gutiérrez and Hintsa is in the category of rules for the layout design for warehouses and terminals. C-TPAT now has guidelines for this, as has been pointed out above. This also seems to be the case with the category “security culture development” where C-TPAT has rules for incentive programmes for employees, partly in rules for importers and partly in the Supply Chain Security Best Practices Catalog. For the categories “information dissemination process” and “organisational roles and responsibilities” the classification is not so easy to make. There is probably an ambition in the C-TPAT programme to create rules and structures for this. The same applies to the category “Prevention, detection and reporting of shipping process anomalies” where the guidelines for importers of March 2005 contain specific instructions on ways in which deviations from declared cargo shall be traced and checked but where there are no rules for ways in which deviations from arrival times and routes shall be followed up. Since this is something of a borderline issue the comparison in the categories has not been revised.

The EU’s AEO programme is more difficult to assess since the system is not yet in operation. The assessment is thus based on the limited information available. Where the categories “Warehouse/terminal layout design” and “Exploitation of cargo and vehicle anti-tampering technical solutions” are concerned there are now rules for dealing with this in the AEO system. For those categories that concern dissemination of information, organisational roles and development of a security culture this is less clear. However, it should be remembered that the entire AEO system is based on controls of the persons who have certain key positions in a company and that part of the work described under these categories is built into the system even if the rules are not as explicit as in C-TPAT. The same can be said to apply to the category “Business partners evaluation system” where there are rules for ways in which business partners shall be treated but no specific system for ways in which they should be selected and no limitations on the companies that can be considered as new business partners. For the category “Prevention, detection and reporting of shipping process anomalies” the same applies as for C-TPAT, i.e. that there are routines for deviations in cargo but there are no rules for tracing deviations in arrival times and routes. We have chosen not to change the assessment of these categories when we make a comparison between the system based on the model of Gutiérrez and Hints, see table 10.3 below.

After this update, the categories in which C-TPAT and the EU’s AEO system do not have similar rules are:

- Rules on warehouse management and control where the AEO system has rules while the C-TPAT lacks rules;
- Surveillance of premises (C-TPAT has rules, AEO lacks rules)
- Quality assurance of information management (C-TPAT has rules, AEO lacks rules)
- Evaluation systems for business partners (C-TPAT has rules, AEO lacks rules).

In this comparison, C-TPAT appears to be the more comprehensive system. A comparison between C-TPAT and the AEO system shows that there are rules for fifteen categories in C-TPAT but only for twelve in the AEO system. In comparison the WCO has 19 categories marked but this

---

is somewhat misleading. This includes rules that do not refer to the WCO’s AEO programme but must be referred to rules for advance notification and other security regulations. In a comparison between the EU AEO system and C-TPAT there is correspondence in twenty of twenty-five categories. Among these categories there are relatively many cases where the reason for correspondence is that there is a lack of rules in both programmes. Similar rules are to be found in eleven categories.

A comparison between AEO in the EU’s programme and the WCO’s framework shows that:

- There is direct correspondence in 15 of the categories. In eleven of these cases there are rules in both sets of rules.
- In cases where there is no correspondence between the programmes there are eight cases of rules in the WCO’s SAFE framework where the EU’s AEO system lacks rules.

A corresponding comparison between C-TPAT and WCO shows that:

- There are corresponding rules in 14 categories and that in a further four categories the programmes correspond with each other in that they lack rules.
- In the seven categories where C-TPAT and AEO do not correspond with each other there are five cases in which the WCO has rules while C-TPAT lacks rules.

All the three programmes correspond with each other in 14 categories. According to this comparison, of these 14 categories there are only eleven categories where there are rules in all three programmes.

<table>
<thead>
<tr>
<th>Security measure</th>
<th>C-TPAT</th>
<th>AEO</th>
<th>WCO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facility Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warehouse/terminal design</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Inventory management and control</td>
<td>-</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>Facility monitoring</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Facility surveillance</td>
<td>x</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Access and presence control</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Cargo management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevention, detection and reporting of shipping process anomalies</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Inspections during the shipping process</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of cargo inspection technical solutions</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Use of cargo tracking technical solutions</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Use of anti-tampering technical solutions</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Personnel</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee hiring/exit process</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Personnel training</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Information dissemination</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Organisational roles and responsibilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security culture development</td>
<td>x</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td><strong>Information management systems</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality assurance of data and information systems</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Protection of business information</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Recordkeeping of shipping information for potential security audits</td>
<td>x</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>Exchange of information with customs authorities</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of international standards for data management</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td><strong>Business network &amp; company management system</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company security management system</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Logistics system designed to reduce risks</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Logistics system designed for rapid recovery</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Business partners evaluation system</td>
<td>x</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Establishment of partnership with customs administration in security matters</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Areas where the programmes have rules. If all three programmes have rules, the title of the area has also been coloured.**

**Areas where there are differences between EU’s AEO and C-TPAT.**

**Areas where there are no rules.**

Table 10.3 Comparison between C-TPAT, the EU’s AEO system and the WCO’s SAFE framework. Produced by the National Board of Trade based on Gutiérrez and Hintsø, (2006).
The comparison is naturally difficult. The American authorities have, as described above, developed a large number of programmes and some of the categories for security work in the model produced by Gutiérrez and Hintsa are covered by other programmes. Thus, for example, the use of technical solutions for cargo inspections is well covered by CSI and the proposal for 100 per cent scanning. The comparison with the WCO is also not entirely accurate since it has been conceived as an ideal system that does not need to take into consideration restrictive legislation where information management is concerned, to mention one example. Likewise it has a broader scope than the two certification programmes included in this comparison.

10.2.2 Conclusions

One conclusion of this comparison is that the requirements stipulated in the AEO and C-TPAT initiatives are not far apart from each other. In many cases the EU has less detailed rules. Perhaps this is due to the fact that the EU’s programme is not yet in operation. There should be good prospects for mutual approval of the two certification programmes. As mentioned above, C-TPAT has explicit rules that state that partner companies engaged by certified companies must be AEO certified or similar in their home countries. Likewise, foreign companies that are invited to participate in C-TPAT must be AEO certified. If the European and American customs authorities should mutually approve certification this would be a major step towards trade facilitation for companies. From both practical and international law perspectives, it would also be of great value if they could recognise each other’s exercise of official powers and delegate certification inspections to the authorities in the country where the company in question is located. Where companies are concerned, it should not be a great amount of work to reuse information and processes that made certification possible in one system or the other. On the other hand, the need for international coordination is greater for those companies that have operations in many countries when the AEO system based on the WCO model is introduced by the customs authorities in more countries.

10.3 Comparison of advance notification rules EU – USA – WCO

In this section a detailed comparison is made between the rules for advance notification of goods in maritime transport in the EU and USA in parallel with a critical examination of the ways in which these rules correspond to the WCO’s SAFE framework. Rules for advance notification have the aim of giving the customs authorities the possibility of analysing and evaluating information in good time before the goods leave the exit country and are intended to make the identification and elimination of potential terrorist threats more effective. To facilitate an in-depth analysis of the rules, a table has been produced (table 10.4) in which the rules for advance notification in the USA, the EU and the WCO are presented. Since the three sets of rules often use different terms for the same concept, one of the difficulties in the analysis has been to determine those elements of information that correspond to each other. The WCO’s secretariat has recently produced a similar table for comparison purposes that has been used as the basis for table 10.4.141

The USA’s rule for advance notification, the Advance Manifest Regulation, referred to hereinafter as the “24 hour rule” is only used for shipments of container freight from ports outside the USA to American ports.142 There are consequently no corresponding rules for exports from the USA to other countries. Since the USA’s SAFE Port Act’s “10+2” programme is not yet legally in force but will probably be adopted in the near future, it has been included in this comparative study to shed light on the ways in which the American rules for advance notification are formulated today and how they may be formulated in the immediate future for maritime transport.

141 World Customs Organization Secretariat “Data Element Comparison” (2007).
142 U.S. Federal Register, Department of the Treasury, Customs Service: “Presentation of Vessel Cargo Declaration to Customs Before Cargo is laden Aboard Vessel at Foreign Port for Transport to the United States”, (2002).
In the EU’s rules for advance notification, which enter into force in July 2009, both entry and exit declarations are required. Requirements in respect of information differ depending on whether it is a case of imports into the Community or exports to countries outside the Community. To make an effective comparison with the USA’s entry requirements in the “24 hour rule”, only the EU’s summary exit declaration is taken up in this comparison. The EU has previously had requirements that exporters shall submit an advance export notification which contains detailed information. This notification will remain in place even when the summary exit declaration is introduced into the system, but will be supplemented by the elements of information required in the summary exit declaration. Companies will thereby avoid duplication of work. Therefore, in those cases where goods are included in the export declaration, there is no requirement for another summary exit declaration. On the other hand, all the new information that has been produced in the summary exit declaration shall be included in the export declaration.

The WCO’s rules for advance notification are the same for imports as exports, but for maritime transport the WCO also has a special cargo declaration that shall be completed. According to the WCO’s guidelines, no more information should be requested for security purposes than that recommended in the WCO’s SAFE framework.

At a first glance at table 10.4 it can be seen that the EU’s exit declaration and the USA’s “24 hour rule” are relatively similar but the EU requires some further information. In their rules for advance notification the WCO and the USA have chosen to merely require information that they consider relevant for security purposes, while the EU has chosen to also include information that must always be submitted to a customs authority, so-called “work flow information”. This refers to data elements such as number of items, goods item number, shipping marks, place of unloading (code), person lodging the summary declaration, declaration date, signature/authentication and location of goods. The EU only requires transport document numbers in those cases where the unique reference number of the consignment is lacking. The final item of information on other special circumstance indicator shall be used to indicate AEO status which can mean that fewer items of information need to be submitted. However, this information does not need to be supplied when it can be deduced automatically or unmistakably from other information submitted by the operator.

These data elements are necessary information that must be submitted in one way or another to the customs authorities in the USA, but at the present time they are not included among the data elements listed in the “24 hour rule”. One reason why the EU, as opposed to the USA, has chosen to include this information in the advance notification is that the EU consists of 27 member states, all with different national systems, where communication between customs authorities must function effectively and where it is thus of great importance that attempts are made at the EU level to make the information as clear, specific and easily accessible between the member states as possible.

If a comparison is then made with the information that is required for security purposes, the USA requires somewhat more information than the EU. While the USA has very detailed information requirements in respect of the carrier and the mode of transport, the EU’s exit declaration lacks requirements in respect of the carrier’s identity, voyage number, vessel name and national flag and merely requires information about the consignor and the consignee of the goods. However, it can be worth mentioning that this information is always required in the export declaration which is submitted in most cases to the customs authority.

In the USA’s “24 hour rule” there are no requirements today in respect of the consignor or exporter of the transported goods. Here there are only requirements in respect of the identity of the carrier and the owner’s representative, which can be considered noteworthy since, in

---

143 In its table, the WCO has also chosen to include the EU’s summary entry declaration.
144 Swedish Ministry of Finance (2007).
146 Source: Mats Larsson, Swedish Customs, 2007.
other respects, the USA requires extremely detailed information. The requirement in respect
of information on the consignor will, however, be included when the SAFE Port Act’s “10+2”
initiative is adopted. Today, the USA’s “24 hour rule” includes 16 of the WCO’s 25 information
requirements, while the EU’s summary exit declaration includes only 12. However, in SAFE
Port Act’s “10+2” further elements of data on the freight will be required which shall determine
whether the container may be loaded onboard the ship. When the container has been loaded
onboard, two further rounds of information will be required: the ship’s vessel stow plan and
“container status message”. Where these new items of information are concerned, neither the
EU nor the WCO has corresponding requirements in respect of six of them. These are detailed
information on the name and address of the manufacturer, consolidator and vendor and the name
and address of the buyer, the location where the container is loaded and the country of origin.

In all three sets of regulations for advance notification, it is prescribed that the information shall be
submitted electronically. The EU and the USA only grant exemption from this requirement under
extremely exceptional circumstances where paper-based declarations are permitted. On the other
hand, the electronic form in which the information shall be submitted is not specified, nor is whether
the information shall be submitted in accordance with the WCO’s Customs Data Model or UN/
CEFACT’s Layout Key. The WCO’s SAFE framework recommends the use of the WCO’s Customs
Data Model. The EU has delegated the responsibility to each member state to decide on which
electronic form they wish to use. In most cases it is a version of EDIFACT which is used for data
communication, but discussions are taking place on using XML instead, which is more modern.
However, this can be a problem for the companies which often have technology for EDIFACT
communication. The EU’s member states communicate with each other with so-called IE messages
via secure networks. The USA uses an EDIFACT standard that is not the same as the EU’s.

In all three sets of rules it is required that the information shall be submitted at least 24 hours before
containers are loaded on board the ship in the exit port. Where this is concerned there are no differences
between the EU, USA and WCO in the information required. The parties that must submit this
information to the customs authorities appear to be the exporter, importer and carrier/shipping company.

From the EU’s regulation it is evident that the responsibility lies with the operator that is responsible
for taking the goods out of the Community, i.e. in most cases the carrier. If a study is made of the
comments on the USA’s “24 hour rule”, it can be seen that it is the carrier/shipping company that
shall supply this information to the customs authority. It is not an unusual phenomenon in the USA
that a carrier or shipping company, which has not succeeded in filling its cargo space on the ship,
hires a competing carrier, a so-called Non-Vessel Operating Carrier (NVOCC). An NVOCC is a
carrier that does not normally engage in maritime transport, but as soon as it is engaged by the
shipping company, becomes its “partner” and has the obligation to submit information 24 hours
before the goods are loaded onboard the ship. Thus both the shipping company and the NVOCC
are obliged to submit information in advance for their respective goods.

In SAFE Port Act’s “10+2” rules, a clear division is made in which the importer shall submit data
elements on the freight and thereafter the carrier shall submit the ship’s cargo plan and “container
status messages”. In the WCO’s SAFE framework there are specific rules that the exporter shall
submit the export declaration and the carrier shall submit the cargo declaration. Here the WCO
thus makes a division of the declaration into two parts since certain information is possessed by
the exporter and other information by the carrier.

Conclusions

One conclusion that can be drawn from this comparison is that the USA’s “24 hour rule” and
the EU’s exit declaration do not actually have decisive differences at the present time in respect

147 Source: Mats Larsson, Swedish Customs, 2007.
148 U.S. Federal Register, Department of the Treasury, Customs Service “Presentation of vessel cargo declaration to
customs before cargo is laden aboard vessel at the foreign port for transport to the US”, (2002), (Vol 67, No. 153).
of the specific information that is required for security purposes. Both the USA and the EU have chosen not to request all the 25 items of information which, according to the WCO, it is possible for them to do. Nor, according to the WCO’s guidelines, should customs authorities request more advance information for security purposes than that included on the WCO’s list. However, the question is whether the USA and the EU comply with this recommendation.

The EU’s rules contain, as described above, ten more data elements with so-called “work flow information”. This should thus mean that the EU exceeds the maximum level stipulated by the WCO. The EU’s advance notification rules also differ from those of the USA and WCO. As opposed to the EU, the WCO and the USA have chosen merely to require information that they consider relevant for security purposes. However, there is reason to question why the WCO has not included the “work flow information” in a supplementary field in its advance notification in order to clarify how these data elements shall be presented in as uniform and coordinated way as possible, for example show how the data elements declaration date and signature shall be given when submitting information.

Today the USA’s “24 hour rule” is within the framework of the WCO’s recommendations. On the other hand, when the SAFE Port Act’s “10+2” rules are adopted, the American rules will exceed by far the maximum list drawn up by the WCO. In addition, the differences between the EU and the USA will be considerably greater. In preparation for the WCO’s council meeting in June 2008, the USA has informally presented a request that the WCO revises its advance notification list and extends it with further data elements that would better correspond to the SAFE Port Act’s “10+2” rules. It is probable that “10+2” will be adopted in 2008 and it remains to be seen whether the USA will await a possible revision by the WCO of its framework agreement or whether they will adopt “10+2” regardless of whatever the WCO decides to do.149

There is a need for a more uniform and harmonised international system in respect of the terminology of the various items of information that are required. Today the USA and the EU often use different designations for information that is largely the same, which creates unnecessary confusion not just when making comparisons but probably also for countries. In its comparative table the WCO has chosen to interpret the different data elements that they perceive as having the same meaning, and has adopted a common term for these elements which makes it easier to understand the table. Ideally in the future the EU and the USA should use these common terms. Moreover it would make things easier for international trade if all parties concerned could agree on one and the same standard for electronic format. As mentioned above, the WCO recommends that the WCO’s Customs Data Model is followed with the aim of standardising and harmonising information requirements and procedures to make the exchange of information more effective between the parties involved in international cross-border transactions.

Where the question of the party that should submit the advance notification information is concerned, the rules of the EU, the USA and the WCO appear to go their own separate ways, and therefore there is a need for international coordination in this respect. The WCO has chosen to clearly divide the advance notification into two different declarations since, in reality, it is usually both the exporter and the carrier that possess different information about the cargo. It is therefore of importance that both complete the advance notification. It is not possible to find this division of responsibilities in either the EU’s summary exit declaration or in the USA’s “24 hour rule”. The EU requires, as mentioned above, that the responsibility for the submission of information rests with the party that is responsible for taking the goods out of the Community. Since this is almost exclusively the carrier, it can be asked why the EU does not instead specify this in the regulation. When the SAFE Port Act’s “10+2” programme is adopted, the USA will make a clear division of responsibilities in respect of who is responsible to submit what information and thus follow the WCO’s recommendations. One conclusion that can be drawn from the above is thus that the EU should clarify its rules as to who should submit what information and make a similar division of responsibilities that corresponds with that of the WCO and the USA.

---

<table>
<thead>
<tr>
<th>Information required</th>
<th>WCQ</th>
<th>EU</th>
<th>US 24-hour rule</th>
<th>US ‘10+2’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporter</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consignor</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Carrier, identity /name</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Importer</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Recipient</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Parties that shall be informed</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination of the goods</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country codes in route order</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent/Representative</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commodity code/description of goods</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UN code for dangerous goods</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of package and number of packages</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total gross weight</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment identification number</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seal number</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total invoiced amount</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unique consignment reference number</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of loading</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity/nationality of active means of transport at border crossings</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference number of transport</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code for payment of transport charges</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit customs office</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code for first place of arrival</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date and time of arrival to 1st place of arrival in customs area</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short description of freight</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturer’s name/address</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor’s name/address</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buyer’s name/address</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place where the container is loaded</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consolidator’s name/address</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country of origin</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of items</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Goods item number</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shipping marks</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of unloading (code)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location of the goods</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Person lodging the summary declaration</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport document number 2)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Declaration date</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature/authentication</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code for other special circumstances</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No information requested

Information that will be requested under the SAFE Port Act and where there are no similar requirements in the WCO or EU
Information requested by the EU, so-called “work flow information” which is not particularly relevant for security purposes.

x = SAFE Port Act (10+2) which has not yet been passed.
1) = According to the WCO this should be described as the port for unloading
2) If there is no unique consignment reference number

Table 10.4 Comparative table of the rules for advance notification between the EU, USA and WCO.
11 Risk analysis of threats to the supply chain

Measures against the threat that terrorists might use a container to transport or deliver chemical, biological or radiological and/or nuclear weapons (CBRN weapons) are high on the priority list of the authorities due to the catastrophic effects that an attack of this type would lead to. A very large number of the security initiatives described in this report have this scenario in mind. This is expressed most clearly in the USA’s initiatives. In a report from the OECD and the European Conference of Ministers of Transport of 2005, the risks from intermodal container traffic are analysed. The authors of the report attach great importance to studying how risk analyses are produced and how they relate to the different security measures. The discussion in the OECD report demonstrates that a consistent risk analysis shows that attacks using CBRN weapons are not so probable. The report presents in detail what should be included in a risk analysis. This section of the report is based in its entirety on the OECD report.

Security measures must be adapted to the ways in which terrorists can possibly be perceived to use the supply chain and containers respectively. Containers are used all the time to smuggle goods, drugs and even people. In addition they are the target of theft. If organised crime has the resources and know-how to circumvent an increasingly rigorous control network from the customs to the police, it is reasonable to assume that well organised terrorists also have this ability. Container traffic has been used for laundering money, transporting suspected terrorists and for providing logistical support for certain attacks. The Liberation Tigers of Tamil Eelam in Sri Lanka is the organisation that has used container traffic most, but there is evidence that Al-Qaeda also used the supply chain to transport bomb components prior to the attacks in Tanzania and Kenya in 1998. In addition there are examples that terrorist groups have used the supply chain and its mechanisms to do legitimate business and in this way generate income for their activities. There is a value in the supply chain for terrorists who can use its normal functions for their purposes. For this reason the incentive to disrupt the supply chain is not as great as it otherwise could be.

It can be asked how well prepared and capable terrorists are to use containers as a platform for a CBRN weapon. However, this does not mean that measures should not be taken to provide protection against this, but rather that measures of this type should rest on a solid foundation of national and international risk assessments. If terrorists want to use the supply chain to deliver a CBRN weapon it could in all likelihood be done in two ways:

Hijacked container: The terrorists enter the supply chain and place the weapon in an existing container transport.

Trojan horse: The terrorist establishes a legitimate business and when, after a period of time, it is subjected to fewer controls, one of its shipments is used for shipping a weapon.

150 “C-TPAT partners have worked with CBP to protect their supply chains from concealment of terrorist weapons, including weapons of mass destruction, and global supply chains are more secure today as a result of C-TPAT.” Commissioner Robert C. Bonner in Prologue to Securing the Global Supply Chain Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan, Washington D.C. USA, November 2004.

151 The ECMT European Conference of Ministers of Transport consists of ministers of transport from 43 member states.

152 OECD/ECMT (2005). Facts and models in this section are based on this report.
Will terrorists use containers to deliver a bomb? It is impossible to know the answer to this question but it should be possible to provide a reasonable answer by making a thorough risk analysis. The OECD report points out that in fact, parts of the risk analysis are not fully implemented. According to the OECD report a risk analysis should contain the following components:

1. Threat assessment: identifies adverse events that can have an impact on the issue at hand. These events can occur at the local, national or global level.
2. Vulnerability assessment: identifies weaknesses in infrastructure or other physical structures, processes, personnel policies or other vulnerabilities that might be exploited by terrorist groups.
3. Criticality assessment: identifies, assesses and prioritises action strategies based on the relative importance of possible targets and impacted systems.
4. Risk assessment: either qualitatively or quantitatively seeks to determine the likelihood of an event occurring (e.g. terrorist use of a container to deliver a CBRN weapon). Also seeks to evaluate the severity and impact of the event.
5. Risk characterisation: seeks to assign risk on a scale (e.g. low, medium, high) and serves as a basis for developing effective responses.
6. Risk mitigation: implementation of counter-measures, taking into account risk, costs and other factors that could have an effect on implementation.
7. Systems approach: a systems approach in risk management of container security vis-à-vis terrorist action should address all areas that have an impact on the issue. This means addressing procedures, actors, technology, infrastructure, infrastructure and policy and governance issues, not only in the field of transport but upstream as well.
8. Monitoring and evaluation: these are continuous assessment processes undertaken to ensure the relevance of current security measures and strategies. These include external peer review, testing and validation.
In the OECD report it is maintained that all these components are necessary for balanced risk analyses and that many countries, when they draw up their security initiatives, even the most ambitious, have shortcomings in their analysis of the likelihood that a container will be used as a platform for a CBRN weapon. The authors of the report are of the opinion that this information is of vital importance, not so much for the security initiatives that are relatively inexpensive to implement as for those that are expensive to implement and have considerable negative impacts on trade. Furthermore, they are of the opinion that the threat varies between different countries and regions and that the risk analyses and measures taken must be adapted in accordance with this. The analysis must at least answer the questions of who the terrorists are and how they might possibly use containers. It is pointed out that while Al-Qaida and the Japanese group, Aum Shinrikyo, have actively tried to arm themselves with CBRN weapons, other groups would perceive this as directly counterproductive to their idealistic goals. It is also emphasised that there is no known event where terrorists have tried to use a container to deliver a CBRN weapon, nor has any averted attempt to use a container in this way been made public. In the light of this it is reasonable to pose the question of whether terrorist groups would ignore the possibility of using the supply chain for their transports and instead use it to deliver a weapon.

The OECD report analyses the probability that different forms of weapons of mass destruction could be used by terrorists.

**Nuclear weapons**

Where nuclear weapons are concerned, the authors of the OECD report state that there are two ways that a terrorist group could come into the possession of a weapon of this type. One way is to buy the weapon, the other is to manufacture it oneself. They are of the opinion that there are so many obstacles to both procedures that it is not probable that a group could acquire a bomb. Preventing a terrorist group from purchasing a bomb is best done through traditional anti-proliferation procedures. In the OECD report it is maintained that these procedures are so robust that this scenario is, to say the least, unlikely. Manufacturing a nuclear weapon is theoretically simple but requires access to certain key components, for example radioactive material. These are also strictly controlled through anti-proliferation measures and it would be expensive, time-consuming and complicated to acquire this material. If, despite this, a group could acquire a nuclear weapon, a container would not appear to be the best delivery platform. A weapon of this type would be a key asset for the group and it is not likely that they would put their investment at risk by sending the bomb in a container. This would have the effect that, for a relatively long period of time, the group would not have control over it, and would possibly detonate the bomb in a situation where the group is not aware of its exact position. Moreover, a number of other distribution methods are available that imply a lesser risk for the terrorist group. Commercial delivery vehicles, passenger ships or bulk freighters all receive less scrutiny.

**Radiological dispersal weapons**

A more likely scenario is that a terrorist group could acquire low active waste, for example from hospitals or nuclear power plants, and combine this with conventional explosives to create a so-called dirty bomb in order to make an area of land unusable for a long time to come. The psychological and economic impact of an attack of this type would probably be considerable. Scanning against radioactivity in relevant hubs is an effective method against this and therefore it is probable that terrorist groups would choose to produce a bomb of this type *in situ* and avoid using container transport.

**Chemical and biological (CB) weapons**

The use of chemical and biological weapons can be analysed in the same way as for nuclear weapons. The risk varies depending upon whether it is assumed that the groups would obtain the material from government controlled sources or be produced by the terrorists themselves.
Even if in some states the procedures are more lax in this field, most ready-made CB weapons are extremely strictly controlled. Furthermore, considerable know-how and special laboratories are required to produce these weapons. The Aum Shinrikyo sect’s attack in Tokyo’s underground can be regarded as relatively unsuccessful since the chemical agent chosen was of inferior quality and linked to a rudimentary dissemination device. This was the case despite the fact that the sect had large financial resources and good access to expertise and laboratories. Furthermore, in the opinion of the authors of the report, the numerous steps in the production process are sensitive to detection and the container is less suitable as a weapons delivery platform, compared for example to a ventilation system in a high-rise building.

The conclusion of the review above is that, reasonably, it is easier to prevent the manufacture of CBRN weapons than to attempt to discover them in the supply chain. However, in this context, tracing radioactivity in the supply chain has a role to play, which the discussion on low active waste above shows. For terrorist groups it is probably better to choose another distribution method than containers, should they acquire a CBRN weapon.

An idea was presented above on two different ways in which terrorists could use a container: the hijacked container and the Trojan horse. The OECD report classifies the measures which emerged after September 11, 2001, and which can be used against these two methods, into five different categories. In the light of the discussion above, the report presents an analysis of the degree of effectiveness of the different methods.

The five categories are:

- Measures seeking to scan or otherwise physically confirm the contents of the container
- Measures seeking to ensure the physical integrity of the container
- Measures aimed at ensuring the security of the container environment as it moves and is handled in the container transport chain
- Measures seeking to track and trace the container in the supply chain
- Measures centred on the provision, and use of, information related to the shipment

The conclusions of this analysis can be summarised as shown in the figure below.

---

**Figure 11.2** The degree of effectiveness of security measures aimed at preventing different forms of illegal use of containers. Based on “Security measures and the hijacked/Trojan horse scenarios” originally published by OECD in Container Transport Security Across Nodes, 2005, OECD/ECMT
None of the categories of measures illustrated in figure 11.2 tackles the different types of threats with the same method. Different types of physical inspections or scanning are naturally the most effective methods but cannot, in practice, be used on more than a small proportion of the transport flow. Here the screening process, which is dependent on information in order to function, plays a major part. The practical and technical difficulties of 100 per cent scanning have been described elsewhere in this report. Ensuring that a container passes through the supply chain untouched and securing the physical environment of containers are effective measures to the extent which terrorists attempt to enter the supply chain and manipulate the content of containers. On the other hand, they have no effect at all if the terrorists have established a legitimate business. Being able to track and trace containers is of course important in order to ensure that containers that have been hijacked can be rapidly discovered when they are missing from the flow or when their arrival is delayed. It is also important to know where a container is in order to be able to remove it from the chain. This means that in cases of terrorist attacks made under the pretext of legitimate business, it is difficult for the tracking and tracing method to be successful. It is even more difficult for customs authorities to use information submitted in the supply chain process to discover Trojan horses. Some anomalies can naturally show security risks, for example when the compilation of background information is matched with the existing threat situation at the time.

To sum up, according to the OECD/ECMT report, the methods that to a large extent are used in the initiatives described in this report are difficult to use to detect a terrorist group that conceals its identity behind a legitimate business activity. There are arguments for maintaining that it is not particularly likely that a terrorist group will use the supply chain as a platform to deliver a CBRN weapon since there are better methods to do this and terrorists can use the supply chain for their own transports or for laundering money. For this reason it can also be questioned whether all the measures that are being implemented today to secure the flow of containers are proportionate. As the OECD shows in its report, part of the risk analysis is not included. In other words there are measures that do not enhance security to any great extent against the stated threats, while they certainly enhance protection against theft and corresponding illegal activities. It is reasonable to assume that all security measures in the supply chain must be assessed in the light of their cost, as well as the protection they actually provide and the threats they are intended to counteract.
Interview with Dan Purtell, security expert

Dan Purtell, president of the Supply Chain Security Services unit of First Advantage Corporation, was formerly responsible for Intel Corporation’s global supply chain security programme. He also took part in the formation of the Customs Trade Partnership Against Terrorism (C-TPAT) security criteria programme and has assisted numerous companies to obtain certification. He served as Chairman of the Transported Asset Protection Association (TAPA), a global association of security professionals from the cargo insurance industry and multinational corporations and has conducted extensive research for this group.

Dan Purtell points out that the biggest challenge corporations face in complying with the C-TPAT programme is obtaining reliable supply chain security practices from their globally outsourced suppliers, formally known as “business partners” both within the Customs Trade Partnership Against Terrorism (C-TPAT) and the Authorised Economic Operator (AEO) programmes. Many companies, according to Mr. Purtell, are doing a good job securing their own factories and their large Tier 1 suppliers, but fail to vet the majority of other suppliers that represent their extended global supply chain. More than 400 companies certified under the programme, equivalent to approximately 7% of all C-TPAT validated companies, have experienced suspensions or have been removed from the programme. Many of the suspensions resulted from unmanifested cargo (drugs or contraband) being introduced into U.S. destined shipments, which were detected by U.S. Customs and Border Protection (CBP) prior to that cargo entering the United States. The remainder of the infractions stem from companies failing to meet security criteria as outlined within the C-TPAT programme.

Dan Purtell states, “U.S. Customs and Border Protection’s detection of unmanifested materials is evidence that their layered security approach and the container inspection targeting programme (both sea containers and trucks/trailers) is an effective and cost-effective way of identifying supply chain risks.”

The fact that contraband is being introduced in some C-TPAT member company shipments, however, is an indicator that companies need to improve risk assessments when it comes to their international supplier base. Many of the exposures that led to these security incidents were preventable with proper business partner risk analysis. Some of the leading security exposures that could lead to the introduction of unmanifested materials into a supply chain include:

- Supplier country of origin risk(s): Western terrorism threat level, cargo tampering rates and the host government’s ability to suppress and control these exposures.
- Lack of contractually mandating that business partners are either C-TPAT certified or compliant with C-TPAT security criteria.
- Lack of a global supplier base risk assessment process, which identifies high-risk business partners.
- Security and cargo “chain of custody gaps” within the supply chain, including un-vetted container stuffing, consolidation or 3rd Party Logistics and in-transit warehouse locations.
- Consolidation of C-TPAT member company materials with non-C-TPAT company materials (consolidated shipments that include unscreened cargo).

Dan Purtell stresses the importance of proper risk analysis when trying to secure the international supply chain. According to empirical analysis within the First Advantage’s Supply Chain Security Services unit, $1.25 trillion is exported from multiple countries that maintain a high or severe anti-Western terrorism level, and approximately $750 billion of this cargo is exported to Western countries, such as the United States and many European Union countries.
This analysis should be an underlying factor when companies plan where to place their production and from where to choose suppliers. He compares Sri Lanka and Indonesia as two interesting examples.

Geographical neighbours, both countries are affected by terrorist activities; however, it is easily and inaccurately assumed that these countries represent the same level and type of risk to international trade. Closer analysis shows a more complex image. As the Liberation Tigers of Tamil Eelam (Tamil Tigers) in Sri Lanka is solely focused on fighting their own government and is classified as a Nationalist group, Jemaah Islamiya (JI) in Indonesia has targeted Western interests and commerce. As confirmed by several governments, JI is responsible for multiple bombings since 2001. These attacks include the Bali nightclub bombing, (which resulted in the loss of 202 lives) and the Australian Embassy and the Marriott hotel bombing in Jakarta. All of these attacks focused on Western targets as noted within JI’s stated objectives and ideologies. Analysis of a terrorist group’s ideologies is critical when identifying exposures within the supply chain. It would not fit within the Tamil Tiger’s ideology to place a dirty bomb in a U.S. bound sea-container; however the same cannot be said about Jemaah Islamiya. First Advantage’s terrorism analysts have classified Sri Lanka’s terrorist activities as a ‘guarded’ threat to Western commerce (second lowest rating), while Indonesia is classified as ‘severe’, the highest rating on First Advantage’s five-point risk scale.

Examination of these countries’ cargo disruption rates reveals that Indonesia also suffers from frequent and serious cargo tampering and disruption, while Sri Lanka’s cargo tampering rate is less frequent and less severe. Given the severe terrorism and cargo disruption ratings associated with Indonesia, the level of supply chain security compliance for cargo exported from this country to Western civilizations should be closely scrutinized. The elevated risk factors within Indonesia, married with a business partner’s poor level of C-TPAT compliance, could lead to a serious security incident within this supply chain. Suppliers operating in this region should be assessed first to determine the level of compliance with C-TPAT security criteria and the identification of chain of custody gaps that could expose a business partner’s cargo to the introduction of harmful unmanifested materials. Understanding the associated country risks within a country, as well as a business partner’s operation, will significantly reduce exposures to multi-national companies that outsource in potentially high risk countries.

In conclusion, Dan Purtell states that potential terrorist activities aimed at the international supply chain could result in a very serious and global economic impact. Layering security controls throughout the international supply chain as implemented by U.S. Customs and Border Protection is best served by countries that are in the process of implementing similar supply chain security programs.

“A risk-based approach to understand business partners and inbound cargo exposures reduces unnecessary inspections and ensures wise utilization of limited customs organizations’ resources,” Dan Purtell concludes.
12 Summary and conclusions

In this report the National Board of Trade has attempted to describe most of the security initiatives that have been introduced or revised after September 11, 2001, that refer to security in the supply chain. The security initiatives can be broken down into certification programmes between companies and customs authorities, initiatives for the collection of information, legal requirements in respect of minimum levels for controls and protective measures, private initiatives against smuggling or theft, and standardisation initiatives. The predominant majority are certification programmes in which companies and customs authorities conclude agreements under which the companies must work with security in the supply chain in a certain prescribed way. In return the companies receive a reduction in the number of controls motivated by security. One important driving force behind this is that the authorities want to restart the supply chain as rapidly as possible after an incident. In a situation of this type the shipments of certified companies can regarded as secure and can pass through the customs rapidly. Some of the certification programmes have been developed from an original focus on smuggling and compliance with the rules, to having a specific focus on preventing terrorism. In addition to this, an adaptation is being made to the WCO’s SAFE framework. The private initiatives, BASC and TAPA, have been developed since 2001 and are now more comprehensive and have a strong position in their respective markets.

The number of initiatives is growing and it is probable that this trend will continue. At the same time there is greater awareness of the necessity and benefits of harmonising the initiatives and of customs authorities recognising the certification programmes and controls of other countries. This is most clearly expressed in the WCO’s SAFE framework. The SAFE framework encourages the design of certification programmes for Authorised Economic Operators (AEO) and, according to the WCO, by November 2007, 74 countries stated that they intend to introduce AEO programmes.

Three points of departure for the security initiatives

There are more or less three points of departure in the security initiatives discussed in this report and they appear to be central themes in all security initiatives. The first refers to securing the capacity for recovery, or the capacity to restore activities after security has been breached. Many certification programmes have strong routines for protection against external threats, often in the form of perimeter protection. Fences around buildings, routines for entry and exit, locks and surveillance are measures that can be found in most of the programmes presented in this report. However, no perimeter protection is entirely secure and therefore routines for recovery when this protection has been breached are very important. The longer it takes to restore production after an incident, the larger the losses will be for the companies concerned and for society in general. This aspect is addressed to a varying degree in the different initiatives, probably partly due to different types of threats and concepts of security in different parts of the world. At the company level, transporters that fulfil certain requirements should experience minimal negative effects after an incident. C-TPAT and the AEO concept in the EU and WCO are examples of this. There appears to be a negative relationship between size and the capacity to recover. The larger a unit is, the more difficult it is to restore operations rapidly after an incident. If the external perimeter protection at a major port has been breached, for example, it is important to avoid a situation in which this paralyses the entire port. The SAFE Port Act and the ISPS code are both initiatives that have been designed to secure ports and the capacity to recovery is a central theme in both these initiatives.

The other central security aspect is the importance of personnel. By introducing technical solutions the systems try to minimise the human factor in modern security systems. All the security initiatives presented in this report have features of high-tech solutions to security problems. Measures to secure the companies’ routines for surveillance and entry and exit controls are based to a large extent on computer systems and high-tech equipment. Security during transport
has also been modernised in recent years. Security seals and the Radio Frequency Identification (RFID) technology have the effect that a container can be checked more easily after it has been packed. However, despite these attempts to minimise the human factor, technical solutions have their limitations. A seal can be loosely attached after having been broken and a RFID seal can lie in a container and still emit a signal. Someone has to pack a container and people will always be necessary to perform this step. In this connection there are strong variations between the programmes. BASC and C-TPAT both contain a large number of measures for ways in which companies shall act towards their employees, and for ways in which this relationship shall be secured in the best possible way. One aspect that is described to a small extent is the question of integrity. In BASC even relatives and friends of employees are investigated.

The third aspect is making use of limited resources in the best possible way by using risk analysis and risk management. The role of risk analysis in security in the supply chain is of central importance when the balance between security and efficiency is discussed. Even if this balance varies between different parts of the world, the goal of more or less all programmes for security in the supply chain is stated to be that trade should be facilitated at the same time as it is secured against external and internal threats. In order to avoid examining all goods in international trade there is a need for instruments for the analysis of risks and threats. Most of the security initiatives have a component which requires risk analysis, and different sets of rules for advance submission of information are methods of providing necessary input for an analysis of this type. The proposed rules for 100 per cent scanning of containers to the USA is the only initiative that completely avoids risk analysis but at the same time it has been the subject of criticism from both the EU and the WCO for constituting a barrier to trade (see further section 4.1.9).

**General economic effects – the effects of the security initiatives on trade**

It is quite clear that international terrorism has considerable negative effects on the international economy, and that the supply chain is sensitive to external threats. The attacks against the USA on September 11, 2001, resulted in a deterioration in the business climate for many companies in the form of increased insurance premiums and costs related to intensified security requirements. Furthermore, terrorism tends to have a negative effect on the flow of trade and investments.

The characteristic of security as a global public good in the international supply chain leads to requirements for coordination between different parties involved, both at the national and international level. There is a risk that investing in national security programmes without harmonising routines and information systems leads to inefficiency and unnecessary costs.

However, it is not merely security that is in focus in these initiatives. Making trade and logistics chains more efficient is an argument that is often used when the benefits of introducing new security measures are discussed. This leads to the question of where the balance lies between security costs and trade facilitation. There are considerable savings to be made through the simplification of customs routines and making logistics chains efficient and most of the initiatives presented in this report lead to both benefits and costs for the various parties involved in the supply chain. The inspection of goods in the supply chain should focus on the consignments that constitute the greatest risk, and in order to determine which consignments these are, effective risk analyses and risk management are required. On the other hand, 100 per cent inspection bears the risk that it will not be possible to realise any benefits from trade facilitation.

More rigorous security requirements can lead, directly or indirectly, to increases in transport times. This leads to an increase in transaction costs. Each day a good is being shipped at sea can be converted into an average customs tariff of 0.8 per cent (See chapter 9). This is the average for trade with the USA. Those who are most severely affected by increases in transport times are probably to be found in places where the cost of transport is already a large proportion of the value of the goods. There is also a risk that intensified security requirements distort competition between regions and change trade patterns since different products are affected in different ways.
by requirements of this type. Therefore it is of great importance to avoid longer transport times as a consequence of stricter security requirements since there is a risk that this will have a negative effect on trade volumes and change international trade flows in an inefficient manner. There is reason to believe that cost increases of this type would have a serious effect on many developing countries, particularly in Africa, since transport costs in these countries are already very high.

The fact that international trade shows a great degree of price sensitivity towards transport costs demonstrates how important it is to minimise the costs arising from intensifying security requirements in the supply chain. The general perception appears to be that as far as possible the security requirements should be based on risk analyses and risk management rather than an increase in the number of inspections. Inspecting all containers can prove to be costly and carries the risk of leading to inefficient solutions for international trade flows.

It is clear that both costs and benefits are distributed asymmetrically among the different parties involved in the supply chain. The economic analysis of the shipping and air transport sectors in chapter 9 establishes that as long as these sectors suffer from overcapacity, the companies will have problems in passing on security-related costs to the final customer.

**Small differences between the certification programmes and advance notification rules of the EU and the USA**

In this report a comparison is made between the EU’s AEO programme, C-TPAT and the regulations in the WCO’s Framework for AEO. One conclusion of this comparison is that the requirements contained in the EU's AEO programme and C-TPAT are fairly close to each other. In 21 of the 25 security categories compared there are rules in both programmes for the ways in which companies should work. In many cases the EU has less detailed rules.

If the European and American customs authorities were to mutually approve each other’s certifications this would represent a step towards trade facilitation for the companies involved. In addition it would be of value if they were able to recognise the exercise of powers by each other’s authorities and delegate certification inspections to the authorities in the country where the company in question is located.

For the companies it should not be a problem to reuse information and processes that have made certification possible in one system or the other. On the other hand the need for international coordination would be greater for those companies with operations in many countries when the AEO system based on the WCO’s model is introduced by the customs authorities of more states.

A summary of the comparison of advance notification rules in the USA’s 24 hour rule and the EU’s summary exit declaration is that ambitions can be seen in both programmes to follow the WCO’s guidelines and recommendations. Differences with respect to the specific information required today for security purposes are not of mayor importance. The differences that exist between the systems lie in the terminology in which different terms are used for the same items of information. In this connection there is a need for greater uniformity and harmonisation in the international system. It would also make things easier for international trade if all parties involved could agree on one and the same standard for electronic communication and a uniform format for electronic documents.

The EU has not to the same extent as the USA and WCO specified the rules in respect of which party that must submit advance information. In order to achieve full correspondence with the WCO’s SAFE framework, a specific breakdown is needed between the information that shall be provided by the exporter and that which shall be given by the carrier.

Today the USA’s 24 hour rule corresponds to the recommendations made in the WCO’s framework. In the near future the SAFE Port Act’s “10+2” rules will enter into force. This means that the USA’s rules for advance notification will greatly exceed the specification of maximum information requirements drawn up by the WCO. Moreover it will mean that the difference between the EU and the USA will be considerably greater. A request from the USA has been
informally presented to the WCO that the organisation should revise its advance notification list and extend it with additional elements of data which better correspond with the SAFE Port Act’s “10+2” rules. A review of the WCO’s SAFE framework may take place at the WCO Council meeting in June 2008.

It is important that the transatlantic dialogue continues and is successful in respect of ways in which the security initiatives in the EU and the USA should be harmonised. The comparison between C-TPAT-AEO-WCO and the advance notification rules shows that there are no considerable differences in substance between the sets of rules, but that it is important that the differences that do exist are harmonised and that the customs authorities on both sides of the Atlantic can recognise each other’s work. In this respect recognition of AEO status in C-TPAT and vice versa is particularly important. At the present time there are no major elements in the submission of information in the EU and USA which are in conflict with the WCO’s SAFE framework. It is likely that the EU and USA can have a decisive influence on the way in which the WCO’s SAFE framework is revised at the regular three-year revisions. In this respect it is important that trade facilitation continues to be in focus.

The advantages and disadvantages of the certification programmes

The analysis of the certification programmes does not provide a completely clear-cut answer to the question of the impact that the programmes have on companies. Many of the studies that have been made of attitudes at companies that participate in the programmes show that there are different perceptions on what the programmes deliver. Benefits that are not due to security, in the real sense of the term, such as fewer thefts, more efficient logistics chains and better relations with customs authorities, are attractive to the companies. Many companies are motivated since, by being certified in one programme, they can gain access to another. Relatively large groups of companies that have responded to questionnaires often point out that they really gain benefits in the form of reductions in security controls. At the same time the number of companies that do not feel that they have received facilitation, or cannot decide in the matter, is usually relatively large.

Where the companies are concerned, the certification programmes will probably become less and less voluntary as demands are made by customers and business partners for participation by companies in the programmes. In this respect the security programmes have similarities with the problems discussed when ISO 9000 was the leading management trend in the 1990s, i.e. that the companies’ rules become inflexible and difficult to change and that only certified suppliers are used. This also applies to the problems when selecting or changing suppliers, documentation etc.

Where the EU’s AEO programme is concerned, it remains to be seen whether it will lead to real trade facilitation for the companies. There will probably be great differences between companies in different member states, depending on the type of relationship they currently have with the customs authorities in their countries.

The certification programmes help the customs authorities to collect information and make risk assessments. However, at the same time they pass on part of the administrative burden to the companies. If the customs authorities issue increasingly detailed rules for this work, the result will be increasingly complicated conditions for the companies. It will also be increasingly important for the authorities to conduct a relevant dialogue with the companies.

Probably there will be real benefits to be gained from the certification programmes when the electronic administration of the customs administration has been introduced in its entirety which can lead to considerably simplified procedures.

The security initiatives and trade facilitation

The four principles of trade facilitation are harmonisation, simplification, standardisation and transparency. The logistical extension of security being a global public good is that harmonisation
between the parties involved is necessary and that all parties involved in the international supply chain are given sufficiently strong incentives to contribute to the public good, i.e. security. One attempt to achieve this is the WCO’s SAFE framework.

Prior to the large increase in AEO programmes that is expected when the WCO’s SAFE framework is put into practice by a large number of states, it is necessary that customs authorities and governments work actively to harmonise and recognise each other’s programmes and that funds are made available for those developing countries that wish to introduce AEO programmes.

Many of the security initiatives state that they have elements of trade facilitation. In a review of the security initiatives it is not always obvious that this is the case. Many of the security initiatives have come into being with a considerable increase in the number of security controls and the certification programmes do not specifically offer a total reduction in these controls even for those companies that reach the highest level of certification.

Advance notification will be introduced in the EU on a large scale for exports, imports and transit goods on July 1, 2009. The procedure includes new operators that must submit information and the rules are not completely definite in respect of what companies must provide which information. This situation should be the same in all countries that introduce AEO programmes. This can hardly be described as a facilitation and the trend indicates an increase in submission of information in the future.

An increase in the information that must be submitted will make great demands in respect of standardisation. It is not only the content of the information that must be harmonised; there must be standards for forms and electronic forms as well as standards for data transmission. The latter is of great importance to facilitate more efficient trade in general.

The major challenge in trade facilitation will probably be in harmonisation and mutual recognition. Even with the WCO’s SAFE framework as a reference, the programmes and rules can differ a great deal. A considerable amount of work remains to be done to ensure that the same type of data is requested and can be transmitted efficiently between the parties involved in the supply chain and the authorities.

It is difficult to obtain proper information on most of the initiatives from the authorities responsible. In a time when the authorities are preparing single window solutions and want to facilitate e-trade there is a great deal of information which is not available on websites or which is contradictory. This does not correspond well with the demands for transparency and accessibility.

USA’s initiative in respect of 100 per cent scanning appears to be in conflict with the idea of trade facilitation and against the principles of the certification programmes. If all containers shall be scanned, it can be difficult to give certified companies special benefits. In the final analysis, the waiting times that will occur before all goods have been scanned and a ship can depart affect all consignments equally.

Critical voices cite shortcomings in security analyses

In a review of the literature that describes the potential effects of terrorist attacks, it is stated that the costs can be very high even if they are difficult to quantify. The economic studies that have calculated the costs of preventing attacks show that investments in security are only profitable, from a strictly economic perspective, if there is a certain percentage risk of a terrorist attack. This is due to the fact that the costs of preventing an attack are high and the risk of an attack on a certain object must therefore be relatively high for the security measures to be financially defensible. The report from OECD quoted in chapter 11 also discusses the importance of risk analyses. The study points out that the probability that a container will be used to transport or deliver CBRN weapons is low and indicates that many initiatives can be ineffective as a method against a container being used to deliver or transport a weapon of mass destruction. The report also argues that the likelihood of a container supply chain being used in this way is very small.


**Trends for security initiatives in the supply chain**

During the work on the analysis presented in this report a number of observations were made. Firstly, the number of security initiatives is clearly increasing. This is partly due to the impact of the WCO’s SAFE framework, and partly since the focus of existing programmes has shifted from smuggling and compliance with rules to security and combating terrorism. This is particularly important when the number of programmes increases – this fact that the number of initiatives is increasing can, in itself, provide reason for concern unless a sufficient degree of harmonisation between the programmes of different countries can be achieved.

Secondly, there is a wish on the part of governments and authorities to take in an ever-increasing amount of information from companies. In this connection there can be reason for vigilance. Producing further information and systems for submitting this information can be costly and it is therefore important that the information really serves its purpose.

Thirdly, 100 per cent scanning of all goods can lead to very long waiting times in ports and other nodes or high costs for new technology. If the USA’s proposal is implemented it would mean a departure from the principle of risk evaluation and selection of high risk objects.

Fourthly, it is difficult to determine without any doubt whether the certification programmes affect trade and, if so, in what ways. It is important that the programmes are designed in such a way that there is a balance between costs and benefits – not just from a business perspective but also from an economic perspective. There are studies that show that there are benefits to be gained by companies from the initiatives, but there are also costs. However, the benefits are directly linked to more efficient logistics management and a reduction in shrinkage. To some extent they are also an effect of more efficient customs processing and fewer controls, even if this is more difficult to quantify. None of the studies presented in this report can clearly demonstrate gains in security.

Fifthly, risk assessments should be better when security initiatives are introduced. There are measures that do not enhance security against the stated threats to any great extent, while in all likelihood they enhance protection against theft and corresponding illegal activities. All security measures in the supply chain must be assessed in the light of their cost and both the protection they actually provide and the threats they are intended counteract.

**Development of world trade – how shall we find a balance?**

In all likelihood, globalisation will continue and intensify. It is not unlikely that this will make completely new demands on security work with the risk that there will be further strains on trade. The security issue will remain topical even in the long term since criminality, political extremism, corruption and ethnic conflicts can be expected to be a part of life in the future. This means that measures to secure the flows of goods and people between countries will continue to remain high on the agenda and thus also affect the possibility of achieving effective trade. Therefore, it is now additionally important to develop the capacity to construct effective and efficient methods and systems that do not distort trade but allocate the costs of security in an effective way and provide clear rules for secure trade. In addition to this there is a risk that security initiatives may be used in the future for protectionist purposes and as technical trade barriers.
References

Published sources

American Association of Exporters and Importers, Business Alliance for Customs Modernization, etc. Letter to Senators Liebermann and Collins, 26 June 2007.


Hummels, D., *Time as a trade barrier*, Purdue University, July 2001.


World Customs Organization, Framework of Standards to secure and facilitate global trade, SAFE, Brussels, June 2005.


**Official sources**


Sweden: Ordinance (1988:146) on the implementation of an agreement between Sweden and the United States of America on mutual assistance in customs matters.

U.S. Federal Register, Dep. of the Treasury, Customs Service, Presentation of Vessel Cargo Declaration to Customs Before Cargo is laden Aboard Vessel at Foreign Port for Transport to the United States, Vol 67, Nr 153, October 2002.

**Non-published sources**


Swedish Ministry of Finance, Memorandum on amendments to the Customs Act and Customs Ordinance, Stockholm, 20 June 2007.
Web documents and websites


www.hm.se


www.tapaemea.com

www.tnt.com


www.wbasco.org

World Customs Organization, About us, http://www.wcoomd.org/home_about_us.htm

Interviews and other direct sources

Lars Karlsson, Director, Capacity Building Directorate, WCO, September-October 2007.

Mats Larsson, Development Strategist, Swedish Customs, November 2007.

Jorge Pérez, Manager, VIMARCO LTDA, Colombia, response to questionnaire, 19 November 2007.


Rolf Stobinsky, Supply Chain Security Manager at H&M, response to questionnaire, 6 August 2007.

Bengt Tufvesson, Regional Security Director, TNT, response to questionnaire, 19 September 2007.
Abbreviations and concepts

ACE: Automated Commercial Environment. CBP’s initiative for electronic submission of information and customs clearance.

ACI: Advance Commercial Information. The Canadian system for advance notification of goods.

AEO: Authorized Economic Operator. Certification of companies that receive advantages in customs and security inspections.

APEC: Asia Pacific Economic Cooperation. An economic forum for countries around the Pacific Ocean, including Australia, Brunei, Chile, Philippines, Hong Kong, Indonesia, Japan, Canada, China, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Russia, Singapore, South Korea, Thailand, USA and Vietnam.

ATS: Automated Targeting System. CBP’s computer system which will comprise part of its electronic customs environment.


BCS: Border Cargo Selectivity. A computer system to determine risk levels and needs of controls in FAST.

CBP: Customs and Border Protection. The USA customs authority which is an agency under the Department of Homeland Security.

CBSA-ASFC: Canada Border Service Protection – Agence des services frontaliers du Canada. The Canadian customs authority.

CCTV: Closed-Circuit Television system. A surveillance TV system.

CSI: Container Security Initiative. A legal initiative in the USA which, among other things, introduced a network of security-certified ports outside the USA, with American customs personnel stationed at the ports.

CSP: Customs Security Programme. The name given to the EU’s rules for AEO and for advance notification. It also includes common control standards, risk indicators and increased cooperation between customs authorities and other authorities inside and outside the EU member states.

C-TPAT: Customs Trade Partnership Against Terrorism. The CBP’s certification programme which is directed towards companies in the supply chain. The companies are certified from the security perspective and are given advantages in customs procedures and security-related controls.

FAST: Free and Secure Trade. An agreement between the USA, Canada and Mexico. The participating countries have agreed to coordinate, as far as possible, their processes for clearance of goods at the borders.

FSR: Freight Suppliers Minimum Security Requirements. An initiative that was introduced when TAPA was established. FSR are requirements placed on general security in the supply chain and which include, for example, perimeter security, premises and security routines.

Green Lane: A procedure that gives certified companies free customs passage apart from random controls.

IIS: Incident Information Service. A service for the exchange of security-related information which TAPA provides for its members.

IMO: International Maritime Organization. A UN agency that has drawn up rules for shipping, ISPS.

ISA: Importer Self-Assessment. A partnership programme for those companies that fulfil CBP’s trade and customs rules.

ISO: International Organization for Standardisation. Develops standards for ways in which the work and management of company processes linked to security should proceed.
**ISPS-Code:** International Ship and Port Facility Security Code. International rules for shipping drawn up by the IMO which contain both mandatory legislation and recommendations.

**Just-in-time production:** Goods that are transported in a carefully calculated way to arrive at the very moment they are needed in production.

**MOU:** Carrier Memorandum of Understanding Programme. Subsequently changed to the Partnership in Protection (PIP) programme. A voluntary Canadian programme that is directed towards preventing crime and terrorism and strengthening security in cross-border trade.

**NII:** Non-Intrusive Inspection. Controls of radioactivity or inspections using X-ray or gamma-ray technology.

**NVOCC:** Non-Vessel Operating Common Carrier. The American designation of a carrier that does not normally engage in maritime transport but which is hired by a shipping company, and becomes its partner, with the same rights and obligations as the shipping company.

**OSC:** Operation Safe Commerce. An American initiative that was started with the aim of providing support to company-initiated research projects to enhance security in the international supply chain.

**PAPS:** Pre Arrival Processing System. A technical solution for handling goods with the aid of bar codes in FAST.

**PAS ISO 17712:** The ISO-standard for high security seals that are to be used for all containers of C-TPAT certified companies.

**PIP:** Partners in Protection. The Canadian customs authority’s certification programme for companies.

**RFID:** Radio Frequency Identification. A technique used in CSI to rapidly ascertain any containers that have been tampered with after loading.

**SAFE:** WCO Framework of Standards to Secure and Facilitate Global Trade.

**SFI:** Secure Freight Initiative. An initiative that has the aim of strengthening the capacity of the American authorities to track and trace nuclear and other radioactive substances at border passages.

**Single Window:** A concept for trade facilitation that refers to a single electronic location for standardised information.

**SOLAS:** Safety of Life at Sea Convention. The basic pillar in the IMO’s work and the most important convention in security at sea.

**STAR:** Secure Trade in the APEC Region. Conferences arranged by APEC on the theme of security for transport and travel.

**TAPA:** The Technology Asset Protection Association. A global association of companies that contribute to exchange information between companies and authorities and which has drawn up security standards, principally for road transports of high-value goods.

**TEU:** Twenty-foot Equivalent Units. A standard measure for containers.

**TSR:** Freight Supplier Minimum Trucking Security Requirements. An initiative which was introduced when TAPA was established with criteria and minimum requirements in respect of security standards specifically directed towards truck transports of goods.

**UNCTAD:** United Nations Conference on Trade and Development.

**WCO:** World Customs Organization.
Appendix 1: CSI-ports

In December 2007 there were 58 CSI-ports. The date on which the port became a CSI port is given in brackets:

North and South America

Halifax, Montreal, and Vancouver, Canada (March 2002)
Puerto Cortes, Honduras (25 March 2006)
Caucedo, Dominican Republic (25 September 2006)
Kingston, Jamaica (27 September 2006)
Freeport, Bahamas (30 September 2006)
Balboa (27 August 2007), Colón and Manzanillo (28 September 2007), Panama
Santos, Brazil (22 September 2005)
Buenos Aires, Argentina (17 November 2005)
Cartagena, Colombia (13 September 2007)

Europe

Rotterdam, Netherlands (2 September 2002)
Le Havre, France (2 December 2002)
Marseille, France (7 January 2005)
Bremerhaven, Germany (2 February 2003)
Hamburg, Germany (9 February 2003)
Antwerp, Belgium (23 February 2003)
Zeebrugge, Belgium (29 October 2004)
Gothenburg, Sweden (23 May 2003)
Felixstowe, Great Britain (24 May 2003)
Liverpool, Thamesport, Tilbury and Southampton, Great Britain (1 November 2004)
Genoa, Italy (16 June 2003)
La Spezia, Italy (23 June 2003)
Livorno, Italy (30 December 2004)
Naples, Italy (30 September 2004)
Gioia Tauro, Italy (31 October 2004)
Piraeus, Greece (27 July 2004)
Algeciras, Spain (30 July 2004)
Lisbon, Portugal (14 December 2005)
Barcelona and Valencia, Spain (25 September 2006)

Africa
Durban, South Africa (1 December 2003)
Alexandria, Egypt (28 September 2007)

Asia
Singapore (10 March 2003)
Yokohama, Japan (24 March 2003)
Tokyo, Japan (21 May 2004)
Hong Kong (5 May 2003)
Pusan, Korea (4 August 2003)
Port Klang, Malaysia (8 March 2004)
Tanjung Pelepas, Malaysia (16 August 2004)
Nagoya and Kobe, Japan (6 August 2004)
Laem Chabang, Thailand (13 August 2004)
Dubai, United Arab Emirates (26 March 2005)
Shanghai, China (28 April 2005)
Shenzhen, China (24 June 2005)
Kaohsiung, Taiwan (25 July 2005)
Colombo, Sri Lanka (29 September 2005)
Port Salalah, Oman (8 March 2006)
Chi-Lung, Taiwan (25 September 2006)
Ashdod (17 September 2007) and Haifa (25 September 2007) Israel
Port Qasim, Pakistan (2 May 2007)
The National Board of Trade

The National Board of Trade is a governmental agency and the central administrative body in Sweden dealing with foreign trade and trade policy. The Board provides the Government with analyses and recommendations.

Within the framework of the European Union, the Board works for an effective Internal Market, an open trade policy in the EU and a strengthened multilateral trading system within the WTO. The Board also acts as ombudsman for free trade and free movement within the EU as partners of the SOLVIT network. This connects governmental agencies across Europe helping companies and individuals caught between differing regulatory systems.

www.kommers.se
Supply Chain Security Initiatives: A Trade Facilitation Perspective