



Date 2004-04-29	Reference number <b>ISO/TC N 997</b>
Supersedes document	

<b>ISO/TC 104</b>  Title: Freight Containers  Secretariat: ANSI	<b>REQUESTED ACTION</b> Circulated to P- and O-members, and to technical committees and organizations in liaison for:  <input checked="" type="checkbox"/> information  <input type="checkbox"/> discussion at: [venue/date of meeting]  <input type="checkbox"/> comments by [date]  <input type="checkbox"/> voting (P-members only: ballot form attached) by  [date]  <i>P-members of the technical committee or subcommittee concerned have an obligation to vote.</i>
---	---

**Title:** UNCTAD Report – “Container Security: Major Initiatives and Related International Developments”

**Source:** United Nations Conference on Trade and Development (UNCTAD)

**Status:** Please be advised that the UNCTAD report is being circulated for information. The report analyzes the various maritime security initiatives that impact intermodal containers, including C-TPAT, CSI, the 24-Hour Rule, and the ISPS Code. The report concludes that, while these and other measures have enhanced security, unresolved issues include: costs and expenses; delays and disruptions; difficulty in implementation of diverse and detailed requirements; and competitive imbalances and marginalization.

Distr.  
GENERAL

UNCTAD/SDTE/TLB/2004/1  
26 February 2004

ENGLISH ONLY

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

**CONTAINER SECURITY:  
MAJOR INITIATIVES AND RELATED INTERNATIONAL DEVELOPMENTS**

*Report by the UNCTAD secretariat*

## TABLE OF CONTENTS

	<u>Paragraphs</u>
A. INTRODUCTION AND BACKGROUND.....	1-4
B. U.S. INITIATIVES .....	5-70
I. Overview over major relevant initiatives .....	6-43
1. Customs Trade Partnership Against Terrorism (C-TPAT) .....	6-10
2. Container Security Initiative (CSI).....	11-17
3. "The 24-Hour Advance Manifest Rule" or "The 24-Hour Rule" .....	18-34
4. U.S. Trade Act of 2002.....	35-41
5. Related legislation and legislative initiatives .....	42-43
II. Contractual redistribution of security associated costs .....	44-46
III. Potential implications for developing countries .....	47-70
1. General Observations .....	47-50
2. Observation relevant to main U.S. measures.....	51
2.1 C-TPAT .....	52-53
2.2 CSI .....	54-61
2.3 24-Hour Rule (as amended by regulations under the Trade Act 2002).....	62-70
C. RELATED INTERNATIONAL DEVELOPMENTS: A BRIEF OVERVIEW .....	71
I. Developments at the World Custom Organization .....	72-76
II. Developments at the International Maritime Organization .....	77-100
1. Responsibilities of Contracting Governments .....	80-82
2. Responsibilities of vessel-owning and/or operating companies.....	83
3. Special provisions applicable to ships .....	84
4. Control and compliance measures .....	85
5. Responsibilities of Port Facilities .....	86
6. Implementation, cost implications and potential impacts .....	87-97
7. Related developments.....	98-100
III European Union Developments.....	101-102
IV. Developments at the OECD .....	103-107
D. CONCLUDING REMARKS .....	108-113
	<u>Pages</u>
Annex I: New standard term contract clauses developed by BIMCO .....	43-46
Annex II: Abbreviations .....	47-48

## A. INTRODUCTION AND BACKGROUND\*

1. Following the events of September 11<sup>th</sup>, 2001, safety and security considerations have been at the forefront of international concerns. The need to enhance security worldwide is recognized by all Governments and industry. As world trade is largely dependent on maritime transport, the security of the maritime transport system has received particularly significant attention. The United States Government, in response to its own analysis of the vulnerability of the maritime transport system, has taken the lead and initiated a considerable number of measures aimed at enhancing the security of maritime traffic, including port, vessel and cargo security. Given that a reported 50% of the value of all U.S. imports<sup>1</sup> arrive in sea containers, much of the focus has been directed at the particular security challenge posed by maritime container shipments and a number of specific measures relevant to container security have been implemented in the form of laws, regulations and voluntary partnership programs.

2. Several International Organisations, including World Customs Organization (WCO), International Labour Organization (ILO) and International Maritime Organization (IMO), have also reacted swiftly to the need for strengthened security measures at the global level and, over the past two years, have been working on a wide range of measures to enhance maritime transport security.

3. Clearly, different sets of rules and measures which have been implemented or are being considered internationally need to be properly understood and their potential impacts on trade and transport, particularly of developing countries needs to be assessed. Against this background, the Commission on Enterprise, Business Facilitation and Development, at its 7<sup>th</sup> session in February 2003<sup>2</sup> and at its 8<sup>th</sup> session in January 2004, recommended that the UNCTAD secretariat should study and analyse the impact of new security initiatives on the international trade and transport of developing countries and disseminate the information.<sup>3</sup>

4. This report provides a first step in this direction, by focusing on the main measures relevant to maritime container security, namely those initiated by the U.S., and by presenting the most important related international developments in context. The aim of the report is to present a clear overview over the new security environment and to offer some preliminary analysis of its potential impacts for the trade and transport of developing countries. In part B of the report, the major relevant U.S. initiatives are presented and some of their potential implications for developing countries are considered. Part C focuses on related international developments, providing a brief overview over the most important initiatives. The report concludes in Part D with some final remarks.

---

\* This report is based on information available on 10 February 2004. All effort has been made to ensure the accuracy of the information provided.

<sup>1</sup> See <http://www.cbp.gov>. For global liner traffic and container port throughput figures, see *UNCTAD Review of Maritime Transport 2003* ([www.unctad.org](http://www.unctad.org)).

<sup>2</sup> See the Report of the Commission on Enterprise, Business Facilitation and Development on its seventh session TD/B/EX(31)/5 - TD/B/COM.3/55, paragraph 9 of the agreed recommendations.

<sup>3</sup> See the Report of the Commission on Enterprise, Business Facilitation and Development on its eight session TD/B/COM.3/64, paragraph 6 of the agreed recommendations.

## B. U.S. INITIATIVES

5. The main U.S. initiatives relevant to maritime container security are the **Customs Trade Partnership Against Terrorism (C-TPAT)**, the **Container Security Initiative (CSI)**, which focus on establishing partnership relations with industry actors and ports, as well as the so-called **"24-Hour Rule"** and recent regulations under the **U.S. Trade Act of 2002** which amend U.S. customs regulations (19 CFR) and are aimed more specifically at obtaining and monitoring information on cargo. The U.S. Customs and Border Protection Service<sup>4</sup> (CBP, hereafter "U.S. Customs") is the relevant government agency in charge of the administration and enforcement of these programs and regulations.<sup>5</sup>

### I. Overview over major relevant initiatives

#### 1. Customs Trade Partnership Against Terrorism (C-TPAT)

6. The Customs Trade Partnership Against Terrorism (C-TPAT) is a joint government-business initiative aimed at building "co-operative relationships that strengthen overall supply chain and border security".<sup>6</sup> It is intended to enhance the joint efforts of both entities in developing a more secure border environment, by improving and expanding the existing security practices. C-TPAT is a non-contractual voluntary agreement, terminable at any time by written notice by either party. Initially, importers, carriers (air, rail and sea) as well as U.S. port authorities/terminal operators and certain foreign manufacturers are eligible to participate in the program. However, it is envisaged to broaden participation to include actors of all international supply chain categories.<sup>7</sup> Applicants wishing to participate need to fill in a *C-TPAT Supply Chain Security Profile Questionnaire* and to sign a *C-TPAT Agreement to Voluntary Participate*. This *Agreement* includes a list of security recommendations/guidelines the applicant undertakes to apply and respect, but also to communicate to his business partners in the supply chain and work toward building the guidelines into relationships with these companies.

7. Recommendations and guidelines have been tailored to different categories of participant to suit different segments of the supply chain. A sea carrier, for instance, when signing the C-TPAT Agreement, agrees to enhance his efforts to improve "the security for the transportation of passengers, crew, conveyances and cargo throughout the commercial process". He accepts to work at establishing, improving or amending his security processes and procedures in accordance with the C-TPAT security recommendations. Importantly, "where the carrier does not exercise control of a production facility, distribution entity, or process in the supply chain, the carrier agrees to communicate the recommendations/guidelines to those entities". These recommendations include tasks such as controlling all access to vessel while in port, identifying

---

<sup>4</sup> On March 1, 2003, the U.S. Customs Service was transferred to the new Department of Homeland Security. The border inspection functions of the Customs Service and other U.S. government agencies with border protection functions were organized into the Bureau of Customs and Border Protection (CBP). Throughout this report, the term "U.S. Customs" will be used to refer to CBP.

<sup>5</sup> **Please note** that relevant sections of chapter 19 of the United States Code (19 U.S.C.) and the corresponding regulations (19 CFR) referred to in this report may be accessed online via the CBP website (<http://www.cbp.gov>, under "legal"). Also available on the website are recent Federal Register Notices amending the relevant regulations. Other Public Laws referred to in this report may be accessed online at <http://thomas.loc.gov>.

<sup>6</sup> For more information, see <http://www.cbp.gov>.

<sup>7</sup> For eligibility requirements, see <http://www.cbp.gov>.

all persons boarding the vessel, ensuring that all manifest/bill of lading submitted for cargo to be shipped are complete and providing this information to Customs, participation in the Automated Manifest System (AMS), visual inspection of all empty containers (to include the interior of the container) at the foreign port of loading, and ensuring that high security seals are affixed on all loaded containers. Another recommendation, which is of particular importance, is the undertaking to ensure that contract companies who provide vessel related services commit to the C-TPAT security recommendations/guidelines as well as periodically review their security commitments to detect weaknesses in security.<sup>8</sup> Upon request, the C-TPAT participant needs to provide documentation to demonstrate compliance with each C-TPAT recommendation.

8. U.S. Customs, on their part, mainly undertake to assist the carrier in his efforts to enhance security and to expedite clearance of cargo at the U.S border. Once a company becomes a C-TPAT member, its risk score in the Automated Targeting System is partially reduced.<sup>9</sup> U.S. Customs also undertake to conduct initial and periodic surveys to assess the security in place and suggest improvements. Relevant *C-TPAT Validation Process Guidelines*, detailing the relevant security criteria, have been published on the U.S. Customs website.<sup>10</sup>

9. C-TPAT operates on the basis of individual "non-contractual voluntary agreement" to implement certain recommendations. The parties are thus expected to use their *best endeavour* to comply with the C-TPAT recommendations and to enhance the security throughout their supply chain, without, however, incurring liability in case of errors or non-compliance. U.S. Customs may remove a company from C-TPAT membership if they determine that its commitment is not serious or that it has intentionally misled Customs.<sup>11</sup>

10. The process was opened in 2002, with strong support from virtually all of the major liner shipping companies.<sup>12</sup> By May 2003, more than 3000 companies had signed up, including 2,119 importers, 20 U.S. port authorities/terminal operators, 410 carriers and 806 brokers/freight forwarders/NVOCCs.<sup>13</sup>

## 2. Container Security Initiative (CSI)

11. The Container Security Initiative (CSI) is another main program concerning ocean going sea containers, which was developed shortly after September 11, 2001.<sup>14</sup> CSI is based on the premise that the security of the world's maritime trading system needs to be enhanced and that it will be more secure if high-risk cargo containers are targeted and screened before they are loaded. The initiative aims at facilitating detection of potential problems at their earliest possible opportunity and is designed to prevent the smuggling of terrorists or terrorist weapons in ocean-

---

<sup>8</sup> For a detailed list of recommendations, see sample C-TPAT Agreements, available at <http://www.cbp.gov>.

<sup>9</sup> As a result, the likelihood of inspections for Weapons of Mass Destruction (WMD) is decreased; see *Container Security: Expansion of Key Customs Programs will require greater attention to critical success factors*, General Accounting Office, GAO-03-770, Washington, July 2003, (hereafter *GAO-03-770, Container Security*) available at <http://www.gao.gov>.

<sup>10</sup> <http://www.cbp.gov>. For sea carriers, the guidelines refer to Conveyance Security, Access Controls, Procedural Security, Manifest Procedures, Personnel Security, Education and Training Awareness and Physical Security.

<sup>11</sup> See *GAO-03-770, Container Security*, p. 15.

<sup>12</sup> J. D. Kimball and F. Wall, *Shipping and the fight against terrorism*, *Journal of International Maritime Law* 9 [2003] 65.

<sup>13</sup> *GAO-03-770, Container Security*, Table 6; see also *US pushes on with next round in CSI bout*, *Lloyd's List*, 24.6.2003.

<sup>14</sup> For further information, see <http://www.cbp.gov>. Apparently, there is no government regulation establishing the CSI requirements, see *WTO Trade Policy Review United States (WT/TPR/S/126)*, para. 21 (<http://www.wto.org>).

going cargo containers.

12. The Container Security Initiative is a four-part program, which involves:

1. establishing security criteria to identify high-risk containers based on advance information;
2. pre-screening those containers identified as high-risk before they arrive at U.S. ports;
3. using technology to quickly pre-screen high-risk containers, including radiation detectors and large-scale x-ray and gamma ray machines;
4. developing secure and "smart" containers.

13. To implement CSI, and in particular its second aspect, U.S. Customs have been entering into bilateral agreements or partnerships with foreign governments. The agreements provide for the deployment at foreign ports of U.S. officers who will have to target and pre-screen U.S. bound cargo containers before they are shipped. U.S. officers are intended to work with host nation counterparts. It should be noted that U.S. authorities offer reciprocity to participant countries, which can therefore send their customs officers to major U.S. ports to target the containers bound for their countries.<sup>15</sup>

14. The goal of CSI is to improve security without, however, slowing down the movement of legitimate trade. Thus, wherever possible container screenings are to be carried out during periods of down time, when containers sit on the docks waiting to be loaded on a vessel and screenings should not, except in rare cases, have to be carried out again in the United States. In the event a cargo container suspected for potential weapons of mass destruction (WMD) is discovered, it will not be permitted to continue on its course to a U.S. port. Moreover, if it is loaded on a ship bound for a U.S. port, that ship will not be allowed access to U.S. territorial waters.<sup>16</sup> It is not clear whether there is any degree of legal recourse available in case of negligence in the course of inspections leading to errors or physical damage to containers.<sup>17</sup>

15. The initial aim of U.S. authorities was to implement CSI at the ports that send the largest volumes of cargo containers into the United States, in a way that facilitates detection of potential security concerns at the earliest possible opportunity.<sup>18</sup> Several mega ports handling a very large volume of containers bound for the United States have signed declarations of principle to join CSI and are at various stages of implementation.<sup>19</sup> U.S. Customs intend, in a second phase, to expand the program to additional ports, still based on volume, location and strategic concerns.<sup>20</sup> In this context, it should be noted that almost 90% of U.S. inbound maritime container trade originates in 30 countries, several of which are small developing nations.<sup>21</sup> For instance,

---

<sup>15</sup> It appears that so far, Japan and Canada have agreed reciprocal CSI agreements and station their own customs personnel in U.S. ports, see <http://www.cbp.gov>.

<sup>16</sup> *GAO-03-770, Container Security*, p.11; also CBP website at <http://www.cbp.gov> (*Frequently asked questions about CSI*).

<sup>17</sup> *The UK Government and the US Container Security Initiative*, Davies Lavery Report No. 14, Kay Pysden and Samuel Pérez-Goldzveig, ([www.davieslavery.co.uk](http://www.davieslavery.co.uk)).

<sup>18</sup> See <http://www.cbp.gov>.

<sup>19</sup> For a list of ports and for further information, see <http://www.cbp.gov>. According to U.S. Customs, the top 20 ports handle approximately 66% of U.S. destined containers. See also table reproduced on page 7.

<sup>20</sup> It appears that it is planned to expand CSI to cover altogether 40-45 strategic ports, *GAO-03-770, Container Security*, p. 9.

<sup>21</sup> Information relates to U.S. Foreign Waterborne Trade, Containerized Cargo (in TEUs) imported into the U.S. in 2002, see [http://www.marad.dot.gov/Marad\\_Statistics/Con-Cnty-02.htm](http://www.marad.dot.gov/Marad_Statistics/Con-Cnty-02.htm). See table reproduced on page 8.

shipments from countries in South and Central America account for almost 10% of all maritime containers shipped to the U.S., but it appears that so far, none of the ports in the region participate in CSI. Shipments from China and Hong Kong however, account for almost 45% of all containers (in TEUs) shipped to the U.S.

**Dates of CSI Bilateral Arrangements and Deployments by Targeted Ports, May 2003**

Country	Port	Date arrangement signed	CSI team deployments in first year	CSI team deployments after first year
<b>Smart border accord</b>				
Canada	Halifax	December 2001	March 2002	
	Montreal	December 2001	March 2002	
	Vancouver	December 2001	March 2002	
<b>Top 20 ports</b>				
Belgium	Antwerp	June 2002		February 2003
China	Shanghai	October 2002 <sup>a</sup>		
	Yantian	October 2002 <sup>a</sup>		
France	Le Havre	June 2002	December 2002	
Germany	Bremerhaven	August 2002		February 2003
	Hamburg	August 2002		February 2003
Hong Kong	Hong Kong	September 2002		May 2003
Italy	Genoa	November 2002		
	La Spezia	November 2002		
Japan	Tokyo	September 2002		
	Nagoya	September 2002		
	Kobe	September 2002		
	Yokohama	September 2002		March 2003
The Netherlands	Rotterdam	June 2002	August 2002	
Singapore	Singapore	September 2002		March 2003
South Korea	Pusan	January 2003		
Spain	Algeciras	January 2003		
Taiwan	Kaohsiung			
Thailand	Laem Chabang			
United Kingdom	Felixstowe	December 2002		
<b>CSI strategic ports</b>				
Malaysia	Klang	January 2003		
	Tanjung Pelepas	January 2003		
Sweden	Gothenburg	January 2003		May 2003

<sup>a</sup> China has "agreed in principle" to join CSI but has not signed a CSI bilateral arrangement.

Source: *Container Security: Expansion of Key Customs Programs will require greater attention to critical success factors*, General Accounting Office, GAO-03-770, Washington, July 2003, Table 5

**U.S. Foreign Waterborne Trade  
Containerized Cargo**

**Calendar Year 2002  
(Thousands of Teu's)**

<b>Country</b>	<b>Total</b>	<b>Export</b>	<b>Import</b>	<b>Rank</b>
China	4,814	887	3,926	1
Japan	1,575	879	697	2
Hong Kong	1,515	317	1,198	3
Republic of Korea	912	424	488	4
Taiwan	877	283	594	5
Germany	625	178	447	6
Italy	610	110	500	7
Thailand	490	114	376	8
Brazil	474	135	339	9
United Kingdom	455	230	225	10
Netherlands	417	173	244	11
Belgium	412	239	173	12
Indonesia	404	129	275	13
India	332	114	218	14
Malaysia	307	62	245	15
France	282	83	200	16
Guatemala	250	102	148	17
Spain	241	78	163	18
Dominican Republic	233	142	91	19
Honduras	233	103	130	20
Philippines	227	83	144	21
Australia	208	125	83	22
Costa Rica	207	78	129	23
Singapore	181	98	83	24
Chile	171	53	118	25
Turkey	152	64	88	26
Colombia	141	67	74	27
Venezuela	134	89	45	28
Israel	125	50	75	29
Ecuador	116	33	84	30
Top 30	17,120	5,519	11,600	
Top 30 % of Total	86.8%	81.0%	89.8%	
Total All Countries	19,729	6,814	12,916	

Source: [http://www.marad.dot.gov/Marad\\_Statistics/Con-Cnty-02.htm](http://www.marad.dot.gov/Marad_Statistics/Con-Cnty-02.htm)

16. As regards the costs of implementation of CSI, it should be noted that while U.S. Customs are paying to deploy their officers and computers in the foreign ports, host seaports need to obtain screening and detection equipment, which is not provided by or paid for by the United States.<sup>22</sup> In some of the mega ports the required technology may already be in place. However, as concerns other ports, CSI implementation requires the host country to provide and finance detectors, IT equipment as well as any other relevant facilities, personnel and training. It is not entirely clear whether these costs will in all cases be borne by way of public funding or by relevant host ports. As for the costs of screening individual containers, it is for the host country to determine which party (i.e. exporter, importer or any other party) is to pay for the direct costs of screening and unloading containers.

<sup>22</sup> See <http://www.cbp.gov>. The cost of the required scanning equipment has been reported to be in the region of \$1-5 million, see OECD Report, *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003, p. 50 ([www.oecd.org](http://www.oecd.org)).

17. An important aspect of CSI, which still requires further clarification, is the question of effective identification of high-risk containers. U.S. Customs are to "establish criteria" in order to identify high-risk containers. In this context, it should be noted that some critical preliminary observations on the current targeting strategy have recently been made by the U.S. General Accounting Office.<sup>23</sup> In a related study on the planned expansion of the C-TPAT and CSI programs, the Office found that in respect of both programs greater attention to critical success factors was required.<sup>24</sup>

### 3. "The 24-Hour Advance Vessel Manifest Rule" or "The 24-Hour Rule"

18. Whereas the C-TPAT and CSI are partnership-oriented programs, other security initiatives focus on the collection of information, in particular cargo-related information. The main such initiative of relevance to maritime container transportation is the so-called 24-Hour Rule, which is closely connected to CSI. U.S. customs regulations now require detailed manifest information in relation to U.S. bound cargo to be provided 24 hours before loading at the foreign port.<sup>25</sup> It is on the basis of the information provided in the manifest pursuant to this new Rule, that U.S. customs officers posted in CSI host are to identify high-risk containers prior to loading.<sup>26</sup>

19. U.S. law and customs regulations impose certain documentary requirements upon vessels bound for the United States. *Inter alia*, vessels destined for the United States and required to make entry must have a manifest meeting certain requirements.<sup>27</sup> U.S. Customs are the competent authority to specify the form and data content of vessel manifests, as well as the manner of production and delivery or electronic transmittal of the vessel manifest.<sup>28</sup>

20. Prior to December 2, 2002, the relevant customs regulations (19 CFR, Part 4<sup>29</sup>) simply required the master of every vessel arriving in the U.S. to have the manifest on board the vessel.<sup>30</sup> Comprised in the vessel manifest had to be a cargo declaration listing all the inward

---

<sup>23</sup> The preliminary observations suggest that while positive steps for improvement have been taken, the CBP's targeting strategy continues to lack key elements of risk management and is not consistent with recognized modelling practices; *Homeland security: Preliminary observations on efforts to target security inspections of cargo containers*, December 2003, General Accounting Office, GAO-04-325T, p. 7 et. seq. ([www.gao.gov](http://www.gao.gov)).

<sup>24</sup> More specifically, GOA found serious weaknesses in three areas: (i) U.S. Customs had not developed a systematic human capital plan for either program; (ii) although U.S. Customs had attempted to create some performance measures, neither program had "developed measures that reflect progress in achieving program goals"; (iii) U.S. Customs did not have "a strategic plan that describes how it intends to achieve CSI and CTPAT goals and objectives and that makes full accountability possible". The report concludes with a number of specific recommendations. See *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770, July 2003 ([www.gao.gov](http://www.gao.gov)).

<sup>25</sup> The final rule, effecting changes to 19 CFR Part 4 has been published in the U.S. Federal Register/Vol.67, No. 211/Thursday, October 31, 2002, p. 66318. Note that some of these provisions have been revised and others added as a result of new regulations under the Trade Act of 2002, which enter into force within 90 days of their publication on December 5, 2003. For the text of these regulations, see U.S. Federal Register/Vol.68, No. 234/Friday, December 5, 2003/p. 68140.

<sup>26</sup> Observations by the U.S. General Accounting Office suggest that the regulations requiring advance submission manifest regulations were initiated in direct response to U.S. Customs' need to carry out the relevant risk assessment at CSI ports, see *Homeland security: Preliminary observations on efforts to target security inspections of cargo containers*, GAO-04-325T, December 2003, p. 18 and 49 ([www.gao.gov](http://www.gao.gov)).

<sup>27</sup> 19 U.S.C. 1431 and 19 U.S.C. 1434.

<sup>28</sup> 19 U.S.C. 1431(d).

<sup>29</sup> Provisions of 19 U.S.C and 19 CFR, as well as recent Federal Register Notices amending the regulations may be accessed online via the CBP website (<http://www.cbp.gov>, under "legislation").

<sup>30</sup> The usual practice was that the manifest was prepared after all cargo had been loaded. See J. D. Kimball and F. Wall, *Shipping and the fight against terrorism*, Journal of International Maritime Law 9 [2003] 65.

foreign cargo on board the vessel regardless of the intended U.S. port of discharge of the cargo.<sup>31</sup> No merchandise would be unloaded until U.S. Customs had issued a permit for its discharge.<sup>32</sup> In cases where the master of a vessel had committed any violation of customs laws, for example by presenting or transmitting a forged, altered or false manifest, he was liable to pay a civil penalty.<sup>33</sup>

21. Following the events of 11 September 2001, new regulations have been adopted with the aim of enabling U.S. Customs to evaluate the terrorist risk of cargo containers.<sup>34</sup> The new regulations, known as the "24-Hour Rule"<sup>35</sup>, require ocean carriers to transmit cargo manifests for cargo being shipped on a container vessel to the United States 24 hours in advance of loading at foreign ports.<sup>36</sup> Transit containers<sup>37</sup> (so-called FROB, Foreign Cargo Remaining On Board), bound for destinations outside the U.S. are equally affected by the Rule. Bulk shipments<sup>38</sup> are exempted from the requirements of the new regulations. As for break bulk cargo, exceptions may be made on a case-by-case basis.<sup>39</sup> It should be emphasized that any container, which is transhipped before reaching its final U.S. destination will have to fulfil the 24-Hour requirements at the last transshipment port. Thus, in case a consignment is cleared under the Rule and loaded onboard a vessel bound for a specific destination but the vessel later diverts to an intermediate port for transshipment, the carrier will have to comply once again with the Rule.<sup>40</sup> As concerns empty containers, it appears that notification of relevant information needs to be provided to U.S. Customs 24 hours before arrival of the vessel.<sup>41</sup>

22. For each container, the manifest must provide a large number of data elements,<sup>42</sup> including, *inter alia*:

---

<sup>31</sup> 19 CFR § 4.7a (c)(1).

<sup>32</sup> 19 U.S.C 1448.

<sup>33</sup> 19 U.S.C.1436(b)

<sup>34</sup> The final rule, effecting changes to 19 CFR Part 4 has been published in the U.S. Federal Register/Vol.67, No. 211/Thursday, October 31, 2002/p. 66318. Note that some provisions have been revised and others added as a result of new regulations under the Trade Act of 2002, which enter into force within 90 days of their publication on December 5, 2003. For the text of these regulations, see U.S. Federal Register/Vol.68, No. 234/Friday, December 5, 2003/p. 68140.

<sup>35</sup> The final rule has come into effect on December 2, 2002, with enforcement being deferred for an additional 60 days. Following this "grace" period, non-complying cargo has been refused loading and "do not load" notices for cargo with incomplete information have been issued.

<sup>36</sup> 19 CFR § 4.7(b)(2).

<sup>37</sup> So called "Foreign Cargo Remaining on Board" ("FROB") refers to cargo loaded in a foreign port and to be unloaded at another foreign port which remains on board during one or several intervening stops in U.S. ports.

<sup>38</sup> Bulk cargo is defined as homogeneous cargo stowed in bulk, i.e. loose in the hold and not enclosed in any container such as boxes, bales, bags, casks, and so on. It can be free flowing articles such as oil, grain, coal, ore which can be pumped or run through a chute or handled by dumping or articles requiring mechanical handling such as bricks, pip iron, lumber, steel beams etc.

<sup>39</sup> Customers wishing to obtain an exemption must send an exemption request in writing to U.S. Customs.

See Final Rule in U.S. Federal Register/Vol. 67, No. 211/Thursday, October 31, 2002/p. 66318 (66321).

<sup>40</sup> See *FAQ on the 24-Hour Advance Manifest Rule* (Q. 16 and 19), [www.cbp.gov](http://www.cbp.gov). See also *US-Customs 24-hour rule*, Phillips Fox, Transport e-Bulletin, April 2003.

<sup>41</sup> See comment in U.S. Federal Register/Vol.67, No. 211/Thursday, October 31, 2002/p. 66318 (66328).

<sup>42</sup> 19 CFR § 4.7a.

- Detailed and precise description of the cargo OR the 6 digit HTSUS (Harmonized Tariff Schedule of the United States);
- Numbers and quantities of the lowest external packaging unit as per bill of lading;<sup>43</sup>
- Container number and (if applicable) seal number;
- Accurate weight of the cargo;<sup>44</sup>
- The foreign port where the cargo is loaded, the last foreign port before the vessel departs for the U.S. and the first foreign port where the carrier takes possession of the cargo;
- The full names and complete, accurate and valid addresses of the consignee<sup>45</sup> and the shipper of the cargo;<sup>46</sup> alternatively, a unique "identification number" for shipper and consignee to be "assigned by CBP upon completion of the Automated Commercial Environment".

23. As the Rule seeks to establish precisely what is carried in every container, the description of the cargo must be precise enough to enable to identify the shapes, physical characteristics and likely packaging of the manifested cargo so U.S. Customs can identify any anomalies in the cargo when a container is run through imaging equipment. Generic descriptions, such as "FAK" ("freight of all kinds"), "general cargo" and "STC" ("said to contain") are not acceptable, as they do not provide adequate information regarding the merchandise. Descriptive clauses, which were commonly used and accepted until recently are not longer acceptable and have to be replaced by more specific clauses.<sup>47</sup>

24. Indirectly, the new requirements affect also bills of lading and other transport documents used in international trade, as carriers need to relate a number of data elements from the relevant shipping documents,<sup>48</sup> including the identity of the "shipper" and "consignee". Although the terms "shipper" and "consignee" are not clearly defined in the U.S. Customs regulations, the relevant provisions make it clear that what is normally required is information about the foreign vendor, supplier, manufacturer ("shipper") and about the person to whom the goods are to be delivered ("consignee").<sup>49</sup> Information on these parties, however, will often not be available on the basis of bills of lading, as transport documents record information on the "shipper" and "consignee" for the purposes of a contract of carriage, rather than for the purposes envisaged by U.S. Customs.<sup>50</sup>

---

<sup>43</sup> In the case of containers, the smallest packaging unit inside a container is relevant, 19 CFR § 4.7a(c)(4)(v).

<sup>44</sup> For sealed containers, the weight as declared by the shipper may be provided, 19 CFR § 4.7a(c)(4)(vii).

<sup>45</sup> 19 CFR § 4.7a(c)(4)(ix), as amended by the regulations under the Trade Act of 2002. For the consignee, a U.S. address must be provided. Where order bills of lading are issued, the names and addresses of the original consignee and of any other notify party needs to be provided. If no consignee is identified on the order bill of lading, a U.S. notify party needs to be provided. In the case of so-called FROB (note 37, above) no U.S. name and address is required. For consolidated shipments, the NVOCC, freight forwarder or carrier may be listed as consignee. For non-consolidated shipments and for each house bill in a consolidated shipment the party to whom the goods are to be delivered in the U.S needs to be listed.

<sup>46</sup> Where freight forwarders contract with carriers under FMC service contracts as "agents" for various shippers, the name and address of the actual original shipper and not that of the freight forwarder is normally required. 19 CFR § 4.7a(c)(4)(viii), as amended by the regulations under the Trade Act of 2002, expressly states that for consolidated shipments, the identity of the NVOCC, freight forwarder etc. is sufficient, but for non-consolidated shipments and for each house bill in a consolidated shipment "the identity of the foreign vendor, supplier, manufacturer, or similar party" is required, together with a valid foreign address.

<sup>47</sup> See U.S. Federal Register/Vol.67, No. 211/Thursday, October 31, 2002/p. 66318 (66324).

<sup>48</sup> E.g. the description and weight of the contents of sealed containers, as declared by the shipper; see 19 CFR § 4.7a(c)(4)(vii).

<sup>49</sup> See fn. 45 and 46, above.

<sup>50</sup> Note the relevant critical comments by the World Shipping Council on this matter, para. 38, below.

25. The information needs to be provided to U.S. Customs by the carrier, not the shipper of cargo. In practice however, this means that shippers must provide the necessary information several days ahead of sailing, whereas in the past manifests were invariably submitted long after the vessel had departed.<sup>51</sup>

26. The international NVOCC (Non-Vessel Operating Common Carriers) community had expressed some apprehension about having to pass on all the relevant information to the ocean carrier, in particular due to confidentiality concerns.<sup>52</sup> Indeed, if obliged to rely on shipping lines to lodge documents with the U.S. Authorities, they would need to disclose the identity of their clients to sea-carriers, their main competitors. In response to this concern, the final Rule gives NVOCCs the possibility of presenting their cargo manifests directly to U.S. Customs, by enlarging the notion of carrier. However, to be recognized as a "manifesting party", NVOCCs must post an International Carrier Bond<sup>53</sup> and have elected to provide cargo manifest information to Customs electronically.<sup>54</sup> Importantly, the term "NVOCC" as used in the regulations refers only to licensed NVOCCs or to NVOCCs registered with the U.S. Maritime Administration. In non-U.S. trades, NVOCCs do not exist as distinct legal entities. Thus, for instance, foreign freight-forwarders of so-called FROB, who are not registered as "NVOCC", would therefore not be able to file manifests in AMS and need to provide the relevant information to the vessel carrier.

27. It should be noted that under the 24-Hour Rule, as published in October 2002, only carriers participating in the Vessel Automated Manifest System (AMS)<sup>55</sup> were required to provide the vessel's cargo declaration *electronically*. Others could present it via old-fashioned paper transferral means. However, under regulations recently promulgated pursuant to the Trade Act of 2002<sup>56</sup>, electronic transmission of manifests through the AMS is now in all cases mandatory.<sup>57</sup>

28. All vessel carriers operating in the U.S. trade thus need to join AMS. Licensed or registered NVOCCs still retain a choice: they can either ask the ocean carrier to file their cargo declarations or use an Automated Thirty Party Service Provider or become participants in AMS allowing direct transmission of manifest to U.S. Customs.<sup>58</sup>

---

<sup>51</sup> *A brave new world*, Containerisation International, April 2003.

<sup>52</sup> See for instance *Forwarders on the boarder*, Containerisation International, April 2003, p.55; *UK forwarders send stark message to US Customs*, Lloyd's List, 6.2.2003.

<sup>53</sup> See Conditions of the International Carrier Bond (19 CFR § 113.64); NVOCCs that choose to file their manifests directly avoid revealing customer details, but must post a US\$ 50.000 bond with U.S. Customs to cover any fines. On some of the concerns of smaller freight forwarders, see also *Forwarders on the border*, Containerisation International, April 2003.

<sup>54</sup> For further details, see <http://www.cbp.gov>.

<sup>55</sup> The U.S. Customs Automated Manifest System (AMS) is an electronic multi-modular cargo inventory control and release notification system, which interfaces directly with Customs systems. It allows AMS participants to transmit electronically their manifest data directly to the Customs for identification and clearance purposes.

<sup>56</sup> On the Trade Act of 2002, see further part B.I.4, below. The regulations have been published in U.S. Federal Register/Vol.68, No. 234/Friday, December 5, 2003/p. 68140. Note that an additional cargo declaration data element is required under the regulations, namely the date of departure of the vessel from the foreign port of lading, see 19 CFR § 4.7a(c)(4)(xv).

<sup>57</sup> See 19 CFR § 4.7, as amended by the regulations under the Trade Act of 2002, which enter into force within 90 days of their publication on December 5, 2003.

<sup>58</sup> The World Shipping Council (WSC), on behalf of the shipping industry, has repeatedly expressed concern about the fact that NVOCCs are not obliged to independently take responsibility for the filing of manifests, but may continue to file through the vessel carrier. It has been pointed out that a vessel carrier has no means of ensuring

29. It must be emphasized that Customs, having analysed the cargo information, do not send "permission to load" messages to carriers to authorize them to proceed with loading. Therefore, in order to avoid risking a penalty, carriers need to delay loading operations for 24 hours after the submission of the manifest to U.S. Customs to be sure that there is no problem with any particular container. Of course, this is, unless a "do not load" message has been sent by U.S. Customs.<sup>59</sup>

30. Upon arrival of a vessel at a U.S. port, in cases where complete advance manifests in accordance with the new requirements have not been received in relation to part of the cargo, U.S. Customs may delay issuance of a permit to unload that cargo; alternatively, unloading of the entire vessel may be delayed, until all required information is received.<sup>60</sup> The position is the same if U.S. Customs have issued a "do not load" message, for instance because the manifest for containerised cargo contained vague descriptive terms, such as "FAK" "consolidated cargo" "general merchandise" or "various retail merchandise" and that cargo has nevertheless been loaded.

31. As far as penalties are concerned, if the master of a vessel fails to provide manifest information or fails to present or transmit accurate and complete manifest data in the required time period or is found to have presented or transmitted any false, forged or altered document, paper, manifest or data to Customs, he may be liable for civil penalties.<sup>61</sup> If a NVOCC, having elected to transmit cargo manifest information to Customs electronically, fails to do so or transmits false, forged or altered document, paper, manifest or data to Customs, he may be liable for the payment of liquidated damages.<sup>62</sup> However, in this context it should be noted that the regulations, as recently amended, take account of the fact that a carrier or NVOCC may obtain cargo-related information from a third party. In these cases, if the presenting party "is not reasonably able to verify such information, CBP will permit the party to electronically present the information on the basis of what the party reasonably believes to be true".<sup>63</sup>

32. Finally, it is important to note that U.S. legislation provides for the release for public disclosure of information when contained in a vessel manifest.<sup>64</sup> The relevant provision does not specify when the information must be released. For security reasons, Customs have decided not to release information from cargo declarations until the complete manifest is filed with them. Indeed, if Customs were releasing the information shortly after receipt, the information might be published even before vessels departed a foreign port. Premature disclosure of information about incoming cargo could, in case of sensitive shipment such as chemicals, raise new security concerns, as on the basis of the advanced information, there might be attempts to steal or destroy such cargo prior or upon its arrival in the United States.

---

whether an NVOCC has in fact filed a manifest in respect of cargo to be shipped on a vessel. See only WSC comments of September 9, 2002 and of August 22, 2003, submitted as part of the consultation process on relevant regulations. The documents are available on the WSC website, [www.worldshipping.org](http://www.worldshipping.org).

<sup>59</sup> See *Updated USCS and Border Protection Advanced Cargo Manifest Rule Information*, <http://www.kline.com>.

<sup>60</sup> 19 CFR § 4.30.

<sup>61</sup> 19 U.S.C. 1436 (b).

<sup>62</sup> 19 CFR § 113.64 (c). See also CBP press release *CBP expands enforcement of the 24-Hour Rule*, May 1 2003. Carriers may be assessed a \$5000 penalty for first violation and \$10,000 for any subsequent violation attributable to the master. NVOCCs may be assessed liquidated damages in the amount of \$5000.

<sup>63</sup> 19 CFR § 4.7(b)(3)(iii). This new provision has been added by regulations under the Trade Act 2002 (see particularly S. 343(a)(3)(B) US-Trade Act of 2002). On the Trade Act, see further part B.I.4, below.

<sup>64</sup> 19 U.S.C. 1431 (c).

33. As an exception to the rule, importers and consignees may, for business reasons, request confidentiality of their identity as well as of their shipper's identity. If these entities wish to withhold this information from release for public dissemination, they have to submit a specific request to the Authorities.<sup>65</sup> It should be emphasized that pursuant to the relevant provision, only the importer, the consignee or an authorized employee, attorney, or official of the importer or consignee can make such requests.<sup>66</sup>

34. The application and enforcement of the new 24-Hour Rule requires the quick and efficient handling and analysis of very significant amounts of information on the part of U.S. Customs. In the longer term, the sustained ability of U.S. Customs to carry out its functions efficiently will be crucial to ensuring that costly delays and congestions will not arise and legitimate trade will not be unnecessarily slowed down.<sup>67</sup>

#### 4. U.S. Trade Act of 2002

35. The U.S. Trade Act of 2002<sup>68</sup> (Trade Act 2002) was signed into law on August 6, 2002 and contains several provisions of importance for those involved in international trade *to or from* the United States.<sup>69</sup>

**S. 343 Trade Act 2002** (as later amended by the Maritime Security Act of 2002)<sup>70</sup> deals with "mandatory advanced electronic information for cargo and other improved customs reporting procedures". Pursuant to this section, the U.S. Secretary of the Treasury is authorized to promulgate regulations providing for the electronic transmission of information pertaining to cargo to be brought into the United States or to be sent from the United States, prior to arrival or departure of such cargo.<sup>71</sup> The section thus provides the legal basis for expansion of the 24-Hour Rule to both *inbound and outbound* transport. Moreover, while the "original" 24-Hour Rule allowed information to be presented either via paper Customs Form or via AMS, under the Trade Act *only electronic submission* of information is envisaged. Importantly, S. 343 of the Trade Act 2002 concerns *all modes of transport* (rail, truck, air and sea transport).<sup>72</sup>

---

<sup>65</sup> 19 CFR §103.31(3)(d).

<sup>66</sup> In January 2003 and at the request of the NVOCC community, U.S. Customs had proposed to amend the regulations to allow, in addition to the importer or consignee, all parties that electronically transmit vessel cargo manifest information directly to Customs to make confidentiality requests, with respect to the identity of the importer, consignee or shipper. The proposal was however withdrawn in August 2003, for lack of "consensus among members of the trade community". For further information, see Federal Register/Vol. 68, N°6/January 9, 2003/p. 1173 and Federal Register/Vol. 68, N°156/August 13, 2003/p. 48327.

<sup>67</sup> See comments submitted by the World Shipping Council as part of consultations on the proposed 24-Hour Rule (September 9, 2002 at p. 6-8), [www.worldshipping.org](http://www.worldshipping.org). In this context, note the recent findings by the U.S. General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770, July 2003 ([www.gao.gov](http://www.gao.gov)) and see fn. 24, above.

<sup>68</sup> Public Law 107-210. For the text of the legislation, see <http://thomas.loc.gov>.

<sup>69</sup> Chapter 4 III A deals with antiterrorism provisions.

<sup>70</sup> Section 108(a) of the Maritime Transportation Security Act of 2002 makes some amendments to s. 343 of the Trade Act of 2002 relating to the reporting of undocumented cargo to the Customs Service and the mandatory advanced transmission of electronic information to the Customs Service. The amendments are mainly, but not exclusively of a technical nature. For the Maritime Transportation Security Act of 2002 (Public Law 107-295), see <http://thomas.loc.gov>.

<sup>71</sup> For the relevant parameters to be taken into account when drafting the regulations see S. 343(a)(3) Trade Act 2002, as amended by S. 108 of the Maritime Transportation Security Act 2002.

<sup>72</sup> For more information on the "24-Hour Rule", see above part B.I.3.

36. The final regulations under S. 343 of the Trade Act 2002, which amend U.S. Customs regulations (19 CFR) including, *inter alia*, the so-called 24-Hour Rule, have recently been published and are set to enter into force in early March 2004.<sup>73</sup> A full overview over the regulations, as applicable to the different modes of transportation and to U.S. export cargo is beyond the scope of this contribution. The main provisions affecting requirements under the 24-Hour Rule applicable to U.S. imports by sea have already been included in the overview over the Rule.<sup>74</sup>

37. However, it is worth emphasizing that the regulations have also modified the original 24-Hour Rule in respect of the manifest information, relating to the shipper and consignee of the cargo. While the modifications seek to clarify the position by introducing more specific language, the provisions continue to cause concern, in particular in relation to consolidated shipments and shipments by foreign freight-forwarders. The World Shipping Council, which has been in general supportive of the 24-Hour Rule - albeit critical on some aspects - had submitted detailed and well-founded comments, as part of the consultation process, explaining why the definition of "shipper" adopted in the regulation was unsuitable.<sup>75</sup>

38. *Inter alia*, the comments point out that the definition, which does not reflect the legal and commercially recognized use of the term, is "not [...] consistent with commercial practice and usage of a bill of lading, and would create substantial confusion with these commercial documents". Moreover, the rule "could require substantial reworking of carriers' commercial documentation systems, would be very burdensome, and – if it were to have any chance of being effective – would require CBP to mandate that all importers provide their carriers with an accurate list of all their suppliers." It is further pointed out that the rule "impermissibly attempts to mandate that a particular person be named on a commercial bill of lading when the carrier may have no relationship with such a person". Also, that the rule "does not accurately represent how "house" bills of lading are issued and filed". Finally, as "the effort to obtain this information through a bill of lading could be easily circumvented by the shipper", it is proposed to find an alternative mechanism to collect the relevant information.

39. Despite these expressions of concerns, the final rule, as adopted in December 2003 has remained substantively unchanged.

40. In relation to maritime U.S. *export* cargo, another provision of the Trade Act 2002 is of some importance and should also be mentioned. **Section 431A of the Trade Act 2002**, which amends the Tariff Act of 1930<sup>76</sup>, deals exclusively with "documentation of waterborne cargo" and applies to all cargo to be exported that is moved by a "vessel carrier" from a port in the United States. The provision imposes a legal obligation on U.S. shippers or, where applicable, NVOCCs, to provide the ocean carrier with a complete set of shipping documents "no later than 24 hours after the cargo is delivered to the marine terminal operator, but under no circumstances

---

<sup>73</sup> The regulations have been published in U.S. Federal Register/Vol.68, No. 234/Friday, December 5, 2003/p. 68140.

<sup>74</sup> Part B.I.3, above. The main changes relevant to sea transport are (a) the need for electronic transmission of manifests; (b) the change to the rule allowing carriers to rely on shipper-provided information; (c) clarification of the terms "shipper" and "consignee".

<sup>75</sup> WSC comments submitted in the course of consultations on proposed regulations under the Trade Act of 2002, August 22, 2003, at p. 5. See also text to fn. 50, above.

<sup>76</sup> S. 343(b) Trade Act 2002. The provision amends the Tariff Act of 1930 by inserting, after section 431, the text of section 431A of the Trade Act 2002. Parts of section 431A have been further amended by the Maritime Transportation Security Act 2002.

later than 24 hours prior to departure of the vessel".<sup>77</sup> Whoever fails to fulfil these requirements shall be subject to civil penalties up to the value of the cargo or the actual cost of the transportation, whichever is greater.<sup>78</sup> The provision further provides that a marine terminal operator may not load or permit the cargo to be loaded unless the carrier confirms that the cargo is properly documented. Finally, vessel carriers are responsible for reporting to U.S. Customs any undocumented or not properly documented cargo that has remained in the terminal for more than 48 hours after being delivered. Such cargo shall be subject to search, seizure and forfeiture. Regulations under S. 431A, which prescribe the time, manner and form by which shippers shall transmit the required documentation and information appear, however, not yet to have been promulgated.

41. Finally, it should be noted that one further potentially important provision, **Section 343A of the Trade Act 2002**, dealing with "secure systems of transportation" has since been repealed by the Maritime Transportation Security Act of 2002.<sup>79</sup> The provision provided the legal basis for the establishment of a joint task force to evaluate, prototype, and certify secure systems of transportation, and more specifically to establish a program to evaluate and certify secure systems of international *intermodal* transport.

## 5. Related legislation and legislative initiatives

42. Apart from these central U.S. security measures and regulations, several other pieces of legislation relevant to cargo and transport security have been adopted or proposed.<sup>80</sup> Most important of these is the **Maritime Transportation Security Act (MTSA) of 2002**,<sup>81</sup> which has already been referred to in connection with the Trade Act of 2002. The Act is designed to protect the U.S. ports and waterways from a terrorist attack and requires area maritime security committees, security plans for facilities and vessels that may be involved in a transportation security incident. While the Act is consistent with the International Ship and Port Facility Security (ISPS) Code, adopted under the auspices of the IMO in December 2002<sup>82</sup>, its requirements go beyond those of the ISPS Code.<sup>83</sup> This has raised fears that shipowners and operators expecting to operate in U.S. waters would be required to have two security plans.<sup>84</sup>

---

<sup>77</sup> S. 431A(b).

<sup>78</sup> S. 431A(e) and (f).

<sup>79</sup> S. 108(c) Maritime Transportation Security Act of 2002.

<sup>80</sup> A Bill for a Port Protection Act of 2003 (HR 1010) was introduced in the U.S. Congress in February 2003. The proposed legislation goes a considerable step further than existing legislation, in that it calls for the physical inspection of all U.S. bound containers. However, it should be emphasized that the proposal, which could seriously disrupt international trade flows, may never develop into binding legislation. For the text of the Bill, see <http://thomas.loc.gov>.

<sup>81</sup> Public Law 107-295. For the text of the legislation, see <http://thomas.loc.gov>. For a good overview, available online, see J.P. Vayda, *Legislative and Regulatory Responses to Terrorism in the United States of America*, <http://www.nb-ny.com> (Publications).

<sup>82</sup> See part C.II, below.

<sup>83</sup> The Act provides for example for the development of a system of foreign port security assessments. It allows U.S. authorities to make a judgement on the effectiveness of the foreign Port State's anti-terrorism measures and, if not satisfactory, to recommend to the foreign government steps necessary to improve the antiterrorism measures in use in the non secure port. In addition, U.S. authorities may prescribe conditions of entry to the United States for any vessel arriving from such a port, or any vessel carrying cargo or passengers originating from or transhipped through that port, see 46 U.S.C. §§ 70108, 70109 and 70110, of the new chapter on Port Security added by S. 102 MTSA 2002.

<sup>84</sup> For reports on industry reactions, see *Ships visiting US may need two security plans*, Lloyd's List, 4.6.2003; *Mixed response to US security rules*, Lloyd's List, 8.8.2003; *Devil is in the detail*, Fairplay, August 7, 2003; *Confusion grows over rules*, Fairplay, October 23, 2003.

However, as concerns requirements relevant to vessels, the final regulations under the MTSA 2002, which were recently published in the Federal Register<sup>85</sup> make it clear that shipowners or operators whose vessels comply with the requirements of the ISPS Code and who hold a valid International Ship Security Certificate are not required to submit a separate security plan under MTSA 2002.<sup>86</sup>

43. Special mention should also be made of the **Public Health Security and Bioterrorism Preparedness and Response Act of 2002**, which was implemented on December 12, 2003. The Act aims at protecting the health and safety of the people of the United States from an intended or actual terrorist attack on the nation's food supply.<sup>87</sup> In particular, the Act requires for any domestic and foreign facilities that manufacture, process, pack or hold food for human or animal consumption in the United States to register with the U.S. Food and Drug Administration (FDA) and for detailed information on every food shipment to be registered with the authorities before arrival. This prior notice has to be given by the U.S. purchasers or U.S. importers or their agents. U.S. authorities have indicated that there would be a considerable grace period to allow exporters and shipping lines to adjust. Also, it appears that efforts are being made by U.S. Customs and FDA to integrate the filing and risk management mechanisms under the MTSA 2002 and the Bioterrorism Act.<sup>88</sup> However, serious concerns have been expressed as to the effect of the legislation on the "business of trade" and, in particular, on small and medium sized exporters, importers and carriers.<sup>89</sup> The World Shipping Council (WSC), representing the world's leading liner shipping operators,<sup>90</sup> and in general supportive of most U.S. anti-terrorism initiatives, has expressed grave concerns about the workability of the proposed rules, in particular in relation to transit cargoes.<sup>91</sup> Moreover, a considerable number of questions and comments submitted by delegations from both developed and developing countries at recent WTO discussions on the U.S. Trade Policy Review<sup>92</sup> express grave concerns about the impact of the legislation. These range from concerns about uncertainty and costs to more general matters, such as the proportionality of the legislation, its compatibility with principles of non-discrimination and the trade restrictive nature of the Act.<sup>93</sup>

---

<sup>85</sup> Federal Register/Vol.68, No. 204/ Wednesday, October 22, 2003/p. 60483. For an overview, see *US Department of Homeland Security Fact sheet: Maritime Security Requirements*, available at <http://www.dhs.gov>.

<sup>86</sup> 33 CFR § 4.104.105 (c) and § 4.104.115(b) and (c). For reports about initial misgivings on the part of U.S. congress about this rule, see *Congress and coast guard divide*, Fairplay, August 7, 2003.

<sup>87</sup> Public Law 107-188. For the text of the Act, see <http://thomas.loc.gov>. See also the U.S. Food and Drug Administration website at <http://www.fda.gov/oc/bioterrorism/bioact.htm>. Further detailed information is also available at <http://www.cbp.gov>.

<sup>88</sup> See CBP comments in Federal Register/Vol. 68, No. 234/ Friday, December 5, 2003/p. 68140 (68143). The interim final rule on prior notice of imported food shipments is available at <http://www.cfsan.fda.gov/~lrd/fr03o10a.html>.

<sup>89</sup> *New US food laws may prove damaging to import trade*, Lloyd's List, 28.2.2003.

<sup>90</sup> See <http://www.worldshipping.org>. The WSC member lines operate more than 90 percent of the liner industry's vessel tonnage serving America's foreign commerce.

<sup>91</sup> The full relevant submission by the WSC is available on the WSC website, at [http://www.worldshipping.org/fda\\_comments.pdf](http://www.worldshipping.org/fda_comments.pdf). See also *US agencies urged to define security roles*, Lloyd's List 9.4.2003.

<sup>92</sup> WTO Report *Trade Policy Review United States* (WT/TPR/S/126), December 17, 2003, available on the WTO website at [www.wto.org](http://www.wto.org).

<sup>93</sup> See the Advance Written Questions on the WTO's *Trade Policy Review United States*, available as part of the relevant documentation on the discussions which took place on 14 and 16 January 2004 on the WTO website ([www.wto.org](http://www.wto.org)).

## II. Contractual redistribution of security associated costs

44. The shipping industry has swiftly responded to the new U.S. security measures and regulations by the production of a set of standard term clauses, for incorporation into voyage and time charterparties, which in turn will be incorporated into bills of lading and other transport documents issued by the relevant carrier. The main purpose of these clauses, produced by BIMCO,<sup>94</sup> is to shift most of the responsibility as well as costs and liability associated with the relevant obligations (including delays and disruptions in relation to vessels calling at U.S. ports) to cargo interests. Importantly, cargo interests may have to bear expenses and costs which arise, for instance from delay or detention of the cargo carrying vessel, but are not associated with their own cargo, but with cargo belonging to another party and shipped on the same vessel.<sup>95</sup> It has also been reported that carriers have started requesting letters of indemnity to pass any potential liability back down the contractual chain with regard to the provision of incorrect or insufficient information.<sup>96</sup>

45. In order to cover administrative costs associated with the additional reporting requirements under the 24-Hour Rule, most ocean carriers have begun to charge between US\$ 25 and US\$ 35 per bill of lading.<sup>97</sup> In addition, some lines are installing an additional post-transmission amendment charge (or correction charge) for cases where amendments are required after manifest have been filed. Global forwarders, too, have been reported as considering to levy charges of between US\$ 25 and US\$ 60 per bill of lading. The European Shippers' Council (ESC) has pointed out that shippers are concerned that surcharges passed on to them may not reflect the actual costs incurred.<sup>98</sup> At the same time, liner companies point out that any surcharges do not reflect all the extra expenses now being incurred, such as additional personnel costs.<sup>99</sup>

---

<sup>94</sup> The Baltic and International Maritime Council. For the full text of the different clauses, see "Features" on the BIMCO website at <http://www.bimco.dk>. See also BIMCO Bulletin – Vol. 98 No 2.

<sup>95</sup> See the broad wording of U.S. Security clauses presented in Annex I. For the full text of the clauses, see [www.bimco.dk](http://www.bimco.dk).

<sup>96</sup> *Port Security: The Export/Import/Transport Industry and the antiterrorist measures*, Davies Lavery, London, Report 24 ([www.davieslavery.co.uk](http://www.davieslavery.co.uk)).

<sup>97</sup> *24-hour rule encouraging prudence*, Containerisation International, April 2003; *Customs & Border Protection gets serious about advance notification*, PBB Global Logistics White Paper, [www.pbb.com](http://www.pbb.com);

<sup>98</sup> *A brave new world*, Containerisation International, April 2003.

<sup>99</sup> *Lines take on extra staff to cope with US cargo clamp*, Lloyd's List, 5.3.2003. One liner company was reported as having taken on a further 45 people to handle the increased work and having required an extra 1400 hours in computer programming time. See also *Shipping Lines confirm hopes for big rate rises*, South China Morning Post, 28.1.2004, where it is reported that leading transpacific shipping lines, such as OOCL may this year charge up to US\$ 1.000 more per box for carrying goods to the U.S.

Name	Activity	Basis	Base fee (USD)	Corrections fee
Danzas	Forwarder	Container	25	
Panalpina	Forwarder	Bill of Lading	40-60	
Kuehne & Nagel	Forwarder	Bill of Lading	35	
OOCL*	Carrier	Bill of Lading	25	40
Maersk Sealand*	Carrier	Bill of Lading	25	40
P&O Nedlloyd*	Carrier	Bill of Lading	25	40
APL*	Carrier	Bill of Lading	25	40
Hapag-Lloyd*	Carrier	Bill of Lading	25	40
CMA CGM*	Carrier	Bill of Lading	25	40
Cosco*	Carrier	Bill of Lading	25	40
HMM*	Carrier	Bill of Lading	25	40
K Line*	Carrier	Bill of Lading	25	40
MOL*	Carrier	Bill of Lading	25	40
NYK Line*	Carrier	Bill of Lading	25	40
Yangming*	Carrier	Bill of Lading	25	40
Hanjin*	Carrier	Bill of Lading	25	40
Evergreen*	Carrier	Bill of Lading	25	40
Shipping Corporation of India	Carrier	Container	25	
Contship Containerlines	Carrier	Container	25	
CSCCL	Carrier	Bill of Lading	25	

\*members of the Transpacific Stabilisation Agreement

Source: OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003, page 49

46. It is clear that security measures add to the transport and logistics costs of exports, which, in many developing nations are already disproportionately high. While security related costs initially affect carriers, the question of who ultimately bears the extra cost depends on the price elasticity of exports to the U.S. Given the low value of many developing countries' exports, it is reasonable to assume that f.o.b. returns will be adversely affected. Moreover, expensive litigation may be required before the effect of standard clauses such as those mentioned above is clear.

### III. Potential implications for developing countries

#### 1. General observations

47. Press reports over the past two years suggest a considerable degree of apprehension on the part of the international business community, although this appears to have somewhat lessened over time, as the practical operation of the different measures has become clearer. An increasing number of ports now participate in the CSI program and it appears that the C-TPAT program has attracted a large and rapidly growing number of participants.<sup>100</sup> It has been emphasized that the 24-Hour Rule, which has been in force for almost a year has been implemented successfully by the international trade community and has not led to the detention of any legitimate shipment.<sup>101</sup> According to a three-month survey carried out by U.S. Customs in early 2003, only a small number of "do not load" messages were sent and, apparently, in all cases the relevant problems were solved so that ships were able to depart as scheduled.<sup>102</sup> Nevertheless, it is clear that the security measures are not without impact.

<sup>100</sup> See part B.I.1, above.

<sup>101</sup> See *USTR's Daily responds to WTO review of U.S. trade policy*, U.S. Mission Daily Bulletin, 20.1.2004, www.usmission.ch.

<sup>102</sup> According to a CBP press release, a review carried out for 2.4 million bills of lading for the period of 2 February to 29 April 2003 revealed that "260 containers with inadequate cargo descriptions were denied loading for violation

48. Participation in the voluntary programs as well as compliance with mandatory regulations and the resulting potential for associated delays and disruptions to supply chains clearly give rise to considerable costs which, directly and/or indirectly affect private parties involved in trade with and transport to the United States. This poses some key questions, in particular as to the distribution of relevant costs and their effect on the ability of small entities, such as ports, carriers, shippers, intermediaries, particularly from developing countries, to participate in international trade on competitive terms.

49. Independently of who ultimately bears the cost of such measures, even the initial costs, which arise in connection with compliance, may prove to be prohibitive for developing countries' exports.

50. The different measures and regulations, which are applicable in relation to all U.S. trading partners, irrespective of their size or degree of development, require a level of equipment, technology and know-how, which is not in every case in place or easy to establish. Potentially, the legitimate trade of developing countries may be adversely affected, due to the inability of particularly small and medium size enterprises within these countries, to effectively comply with the new requirements. Concerns have been expressed that some of the measures may create non-tariff barriers to trade and the proportionality and effectiveness of some measures has been called into question.<sup>103</sup>

## **2. Observation relevant to main U.S. measures**

51. In relation to the three main security measures discussed in this report, some of the potential issues of concern arising for developing countries are set out below.

### **2.1 C-TPAT**

52. The C-TPAT program establishes for participants a special relationship with U.S. Customs. Participation in the program is currently open to carriers, as well as to U.S. importers and port authorities, but it is envisaged to broaden participation to include all international supply chain categories. The program requires trading partners to work with their service providers throughout the supply chain to enhance security processes and procedures. Various aspects of each stage of the supply chain must be monitored, including employees and the origin of goods. Effective implementation of the agreed recommendations and guidelines requires substantial effort on the part of individual C-TPAT participants. Participants have to invest in the physical integrity of their premises and ensure their trading partners do so as well. Moreover, organisational changes may be required, as well as additional personnel and training, both to improve security and to process relevant paperwork.<sup>104</sup>

53. While large companies may be able to cope with the implementation requirements and the associated costs, for small companies, particularly from developing countries, the requirements

---

of the 24-Hour Rule", but "most of these violations were resolved in time for the shipment to make its original voyage", *CBP expands enforcement of the 24-Hour Rule*, May 1, 2003.

<sup>103</sup> See the Advance Written Questions on the WTO's *Trade Policy Review United States*, available as part of the relevant documentation on the discussions which took place on 14 and 16 January 2004 on the WTO website ([www.wto.org](http://www.wto.org)).

<sup>104</sup> See also OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 ([www.oecd.org](http://www.oecd.org)), p. 52.

resulting from the C-TPAT program may pose difficult new challenges leading to their possible further marginalisation.<sup>105</sup> Small entities may not be in position to face additional expenses to meet the C-TPAT requirements, as the required expenses may be disproportionate to their company's size and financial capacity. However, to maintain any existing business with the United States, they may, in the longer run, not have much of a choice. Although the program is voluntary in nature, in the longer term, participation in the C-TPAT program may be expected of all parties involved in U.S. Trade, including foreign manufacturers, so that failure to participate may lead to competitive disadvantages.<sup>106</sup> U.S.- based importers, carriers and brokers are likely to choose supply partners that can produce reliable and suitable information on their products, organisational structures and procedures. This might exclude some ill-equipped, though trustworthy suppliers in developing countries who lack the means of implementing the relevant C-TPAT recommendations and guidelines.

## 2.2 CSI

54. One of the main concerns in relation to CSI has been pointed out by the European Commission<sup>107</sup>, namely that CSI distorts competition between ports. By signing CSI agreements, ports obtain immediately a "preferred" status, as they are the only ports from which goods may be dispatched to the United States without being liable to encounter import-related problems or delays. Shippers willing to continue exporting to the United States are thus induced to ship from a CSI port and, in consequence, CSI ports are likely to attract more shippers, and also more carriers or freight forwarders. Not every port, however, may be eligible to join the program<sup>108</sup> or be financially in a position to obtain CSI status.

55. While the direct costs associated with participation in the CSI program are difficult to quantify, the preliminary findings of a recent OECD study may serve as a useful guide. According to the OECD, "the direct costs of participation include the purchase/upgrade of container scanning systems if existing container scanning capacity is not sufficient. Container scanners can cost between USD 1-5 million (...). Depending on the nature of port management and national Customs arrangements, these costs can be borne by any number of parties ranging from national governments, local port authorities (government or private) and commercial terminal operators. Furthermore, any of the previously mentioned parties may, or may not, put in place cost-recovery mechanisms such as container surcharges, scanning fees, port duties, etc."<sup>109</sup>

56. Non-CSI ports may find it difficult to stay competitive and, as far as U.S. trade is concerned, may sooner or later be used only for pre-carriage purposes, goods being loaded at one of these ports on feeder vessels to join the nearest CSI port. In the longer term, the Container Security Initiative could thus have significant consequences for non-CSI ports. Competition between ports is already very keen. Big ports keep extending their premises to stay in the lead, small ports try to survive by providing new services and in general all ports try to keep up with new technology and attract new clients. With the introduction of CSI agreements, being

---

<sup>105</sup> See also OECD Economics Department Working Paper No. 334, *The economic consequences of terrorism* (ECO/WKP(2002)20), 17.7.2002 (<http://www.oecd.org/eco>), Box 8. Also published in *Ports and Harbours* (2002).

<sup>106</sup> See also OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 ([www.oecd.org](http://www.oecd.org)), p. 52.

<sup>107</sup> See also para. 60, below.

<sup>108</sup> See "Minimum standards for CSI expansion", at [www.cbp.gov](http://www.cbp.gov), according to which ports *inter alia* must have regular substantial and direct container traffic to U.S. ports.

<sup>109</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 ([www.oecd.org](http://www.oecd.org)), p. 50.

categorized as a "secondary" port may well lead to the general reduction of port activity and therefore to the decline of any non-CSI ports.<sup>110</sup>

57. By the same token, competitive imbalances may be created for shippers and carriers who, in order to avoid the risk of serious delays, need to adapt their operational practices to arrange for shipments through CSI ports and thus face additional costs associated with pre-carriage or re-routing and additional storage. In some instances, countries may find their business become increasingly dependent on foreign ports, thus raising the costs of exports.<sup>111</sup> As concerns different CSI ports, too, importers and exporters may, potentially, find more favourable conditions in one port, rather than another and may therefore decide to adapt their trading patterns in order to avoid additional costs.

58. In view of concerns about possible competitive imbalances between ports within their territories, some States and regions have initiated bilateral co-operation agreements with the U.S. For instance, Canada and the U.S. have signed a "smart border declaration" which outlines a 30-point action plan providing "for on-going collaboration in identifying and addressing security risks while efficiently expediting the legitimate flow of people and goods across the Canada-U.S. border".<sup>112</sup> Customs related action items include in particular harmonized commercial processing, clearance away from the borders, joint facilities and in transit container targeting at seaports.

59. The New Zealand Government, in an effort to avoid any competitive disadvantage of the CSI initiative to any of its individual ports, appears to be working towards a nation-to-nation agreement with the U.S., intended to substitute any otherwise relevant port-specific CSI agreements. It has been reported that the planned compromise agreement would, for instance, involve checking and sealing the containers at loading ports instead of at point of origin and the use, at all minor ports, of portable x-ray machines. The compromise may ensure that small ports would meet the U.S. new requirements and reduce competitive imbalances inside New Zealand.<sup>113</sup>

60. The European Commission, although agreeing in principle with CSI, has initially opposed the initiative, considering that by making an initial selection of a few large European ports for CSI participation, U.S. Customs was pushing EU ports into unhealthy competition with each other. This would invariably lead shippers to divert trade from non-CSI ports and therefore cause a trade-distortion within the EU.<sup>114</sup> The European Commission together with the U.S. Customs Authorities have therefore decided to work on an agreement, which would cover the whole of the

---

<sup>110</sup> For similar consideration, see *Opinion of the European Economic and Social Committee on the Security of Transports*, (2003/C61/28), Official Journal (OJ) C61/174, 14.3.2003, (<http://europa.eu.int/eur-lex>) at para. 5.4 and OECD Economics Department Working Paper No. 334, *The economic consequences of terrorism* (ECO/WKP(2002)20), 17.7.2002 (<http://www.oecd.org/eco>), Box 8. Also published in *Ports and Harbours* (2002).

<sup>111</sup> See the Advance Written Questions on the WTO's *Trade Policy Review United States*, available as part of the relevant documentation on the discussions which took place on 14 and 16 January 2004 on the WTO website ([www.wto.org](http://www.wto.org)).

<sup>112</sup> "U.S.– Canada Smart Border Plan". For more information, see the Canada Border Services Agency website at <http://www.cbsa-asfc.gc.ca>.

<sup>113</sup> *Wellington seeks box compromise*, Lloyd's List, 24.6.2003.

<sup>114</sup> The European Commission has launched infringement procedures against 8 EU Member States that had signed declarations of principle with the U.S. Customs Service. Container traffic from relevant ports covers approximately 85% of maritime container traffic from EU to U.S.A. Although the infringement proceedings are still pending, the Commission will reconsider the position when Customs co-operation under the 1997 EU-U.S. Agreement is legally expanded to cover these aspects. For further information, see [http://europa.eu.int/comm/taxation\\_customs](http://europa.eu.int/comm/taxation_customs).

European Community. An agreement expanding the existing *Agreement on customs co-operation and mutual assistance in customs matters*<sup>115</sup> to include co-operation on "Container Security and Related Matters" was finally initialled in November 2003 and is expected to enter into force in early 2004. The agreement applies to all maritime containers, whatever their place of origin, that are imported into, transhipped through, or transiting the European Community and the United States. It further provides for the expansion of the CSI to all ports in the European Community that meet relevant requirements and for the promotion of comparable standards in the relevant U.S. ports.<sup>116</sup>

61. A concern, which may arise particularly for smaller developing countries, is that in the longer run, a trend towards co-operation agreements such as those mentioned, might trigger a new era of protectionism with global trade being conducted more along the lines of bilateral agreements dividing nations into favoured and less favoured trading-partners.

### **2.3 24-Hour Rule (as amended by regulations under the Trade Act 2002)**

62. This measure, applicable to all containers loaded onto vessels destined for U.S. ports, is probably one of the most contentious of all the security measures.<sup>117</sup> The introduction of the new advance manifest requirements has led to some significant operational changes and adjustments in the trade and transport industry and has serious cost implications. The following examples, while not comprehensive, illustrate the situation:

63. So-called "late gates" practices, which allowed shippers to bring their containers to the port 12 or even 6 to 8 hours before sailing are no longer possible and ports and companies used to operating on that basis have had to adjust.<sup>118</sup> The new rules have reduced liner operators' flexibility to switch a container from one ship to another<sup>119</sup> and to divert a vessel during the voyage to an intermediate port. Carriers, in order to avoid difficulties associated with the 24-Hour Rule have also had to consider reorganise their routing, for instance in relation to U.S. transit cargo, which may now be sent directly to its destination, without calling at U.S. ports.

64. As had been pointed out by the World Shipping Council (WSC), the fact that the Rule also applies to "Foreign Cargo Remaining on Board", i.e. to transit cargo "may have significant operational and vessel deployment ramifications" and will "cause significant difficulties to many foreign shippers, who may not be doing business in or with anyone in the United States".<sup>120</sup>

65. Booking container space on a vessel remains, in many cases, a slow manual process (with the exception of some large shippers and freight forwarders) and the requirements of the 24-Hour Rule have moved up several of the steps in a booking cycle. The number of manifest filings and the associated workload has increased significantly, in some cases by several orders of magnitude.<sup>121</sup> This imposes costs on carriers who must field sufficient clerical/data entry staff to

---

<sup>115</sup> The original agreement was signed on 28 May 1997 and focuses on classical customs co-operation.

<sup>116</sup> For the text of the initialled agreement, see [http://europa.eu.int/comm/taxation\\_customs/index\\_en.htm](http://europa.eu.int/comm/taxation_customs/index_en.htm).

<sup>117</sup> Note only the numerous public comments reflected in U.S. Federal Register/Vol.67, No. 211/Thursday, October 31, 2002/p. 66318 and Vol.68, No. 234/Friday, December 5, 2003/p. 68140.

<sup>118</sup> *Maersk executive warns on security-induced bottleneck*, Lloyd's List Maritime Asia, September 2002.

<sup>119</sup> *Lines take on extra staff to cope with US cargo clamp*, Lloyd's List, 5.3.2003.

<sup>120</sup> See The WSC comments on proposed advance cargo manifest rulemaking, September 9, 2002, at p. 15 (<http://www.worldshipping.org>).

<sup>121</sup> See The WSC comments on proposed advance cargo manifest rulemaking, September 9, 2002, at p. 9. (<http://www.worldshipping.org>). Several examples are provided, e.g. that of a vessel service from Australia, in

handle bookings 24 hours a day and seven days a week.<sup>122</sup> According to an early estimate by one major ocean carrier, an additional US\$ 15 million would be required by that company alone to cover new systems, operating costs and personnel.<sup>123</sup> In order to comply with the advance manifest requirements, carriers require all relevant cargo information 24 to 72 hours before the filing deadline. In fact, although only cargo related *data* needs to be provided a minimum 24 hours before loading, a survey amongst shippers has found that 15% of shippers also provide their loaded containers early. "Shippers blamed resulting delays on shipping line diktats, requiring cargo data to be filed ahead of the U.S. Customs 24-hour deadline, plus 'uneven support' by foreign suppliers, and 'internal barriers to data flow revision'".<sup>124</sup> The same survey found that 30% of shippers are building buffer periods in their logistics operations, in order to avoid any fines and delays.<sup>125</sup> In some congested ports, the additional influx of containers needing temporary storage has entailed costs and in the longer term, there is a risk of generating bottlenecks within port facilities. More generally, concerns continue to be expressed that the 24-hour pre-loading requirement could disrupt "Just In Time" delivery systems.<sup>126</sup> Finally, cargo consolidators of LCL traffic have also been significantly affected by the new requirements as their costs have risen considerably and the speed of loading operations has been reduced.<sup>127</sup>

66. No clear estimates of the overall costs of the 24-Hour Rule have, so far been published. An OECD report prepared only a few months after enforcement of the Rule began refers to early estimates by analysts of US\$ 5-10 billion per year.<sup>128</sup> The report itself concludes that a more realistic estimate, based on documentation fees levied by carriers to cover their administrative costs and annual TEU import figures, may be in the region of approximately US\$ 281.7 million.<sup>129</sup> However, it should be noted that the documentation fee (of typically US\$ 25 per TEU) does not cover the variety of costs associated with any potential delays, liabilities and fines,

---

respect of which under the old rules [including U.S. Coast Guard requirements] only one inward manifest was required 48 hours before arrival in a U.S. port. As the vessel might stop at many intermediate ports during its voyage of several weeks, the new requirement of manifest filing 24 hours ahead of loading at each foreign port means that more than 10 manifest filings could be generated in relation to the single sailing. It is further stated: "A single weekly trans-Pacific service that calls at five Asian ports would generate 260 annual filings by a single vessel carrier offering that service. A substantial number of vessel carriers would each have thousands of foreign load port manifest filings a year".

<sup>122</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 (www.oecd.org), 47. On concerns about administrative costs, see also *Security vs. supply chain*, Containerisation International, April 2003.

<sup>123</sup> See The WSC comments on proposed advance cargo manifest rulemaking, September 9, 2002, at p. 21 (<http://www.worldshipping.org>). Cost items specifically mentioned in the comments include (depending on the carrier) systems re-engineering, new software, new hardware and enhancements to computer systems, as well as training agents, sales and marketing personnel, and terminal operations personnel.

<sup>124</sup> *Bespoke delays follow 24-hour Rule*, Financial Times, February 24, 2003, reporting on the results of a survey carried out by logistics operator BDP International.

<sup>125</sup> It should be noted that according to U.S. Customs, several weekly hours of computer "down-time" are scheduled which carriers need to take into account when calculating the time frame in which to submit their cargo manifests. See *Frequently Asked Questions* (No. 27) at <http://www.cbp.gov>.

<sup>126</sup> See comments on the submission time frame for maritime cargo, which were submitted as part of the consultation process on recent regulations under the Trade Act 2002, Federal Register/Vol. 68, No. 234, Friday/December 5, 2003/p. 68140 (68145).

<sup>127</sup> *Security vs supply chain*, Containerisation International, April 2003.

<sup>128</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 (www.oecd.org), p. 48, citing "Ten billion dollar costs for 24-hour Rule", CI-online, March 12, 2003.

<sup>129</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 (www.oecd.org), p. 48.

which may arise in relation to the 24-Hour Rule.<sup>130</sup> These costs and expenses, which may, in the longer term, be significant, are likely to be passed on to cargo interests by way of standard contract terms, as has already been mentioned in this report.<sup>131</sup>

### *Electronic filing requirements according to regulations under the Trade Act 2002*

67. As has been pointed out above, under new regulations, promulgated under the U.S. Trade Act of 2002, electronic submission of manifest through the AMS is now mandatory for all parties, i.e. for vessel carriers and for NVOCCs who elect to participate in AMS. A regulatory impact assessment conducted by U.S. Customs in November 2003 concludes that the economic impact of the electronic filing requirement in relation to maritime transport would be negligible, as most carriers owned by U.S. citizens or registered under the U.S. flag already use the AMS.<sup>132</sup> Only about 100 foreign carriers who move cargo into U.S. ports did not yet use AMS. However, despite this, it appears that outside the U.S., concerns persist, within the shipping and particularly within the NVOCC community, as to the financial impact of the electronic filing requirement.<sup>133</sup> For instance, one comment submitted in the course of consultations on the proposed rule states:

"It is estimated that 25 million bills of lading are issued annually for container cargo from Japan to the United States. Shipping companies are charged a \$25 fee<sup>134</sup> for transforming and inputting a shipper's cargo data to the AMS. This means that the cost of trade between Japan and the United States will increase \$625 million per year through the introduction of the 24-hour rule. Contrary to the CBP's claim that much of the trade already uses electronic transmission systems and therefore would not incur significant compliance costs, this fact indicates that substantial costs would be on the trade when the requirements of advance electronic cargo information are implemented".<sup>135</sup>

68. For developing countries, the considerations underlying the comment are clearly of particular concern. In addition to any potential financial impact of the electronic filing requirements, there may, however, be other repercussions. The regulatory requirements may further a trend to move to an electronic environment throughout the supply-chain. In the longer run, this is likely to increase efficiency and reduce costs. However, it also requires the availability of reliable equipment, technical assistance, know-how and, not least, electricity supply. For the time being, this is a problem in many developing countries and there is thus the risk that exporters may find it increasingly difficult to participate competitively in international trade.

---

<sup>130</sup> For instance, U.S. Customs may delay issuance of permit to unload the entire vessel even if only a small proportion of the cargo is found to be non-compliant. For shippers and consignees, who complied with the requirements but find their cargo on the same vessel as a non-compliant cargo, the consequences may be significant. They will have to wait until all required information for the non-compliant cargo is received before the vessel is finally unloaded. This delay may generate additional losses, for example extra expenses for container hire or loss of business in connection with sub-sales.

<sup>131</sup> Part B.II, above.

<sup>132</sup> CBP, Department of Homeland Security, *Regulatory Impact Analysis Advanced Electronic Filing Rule*, November 13, 2003 (<http://www.cbp.gov>), p. 53.

<sup>133</sup> See the various specific comments submitted as part of the consultation process on recent regulations under the Trade Act 2002, Federal Register/Vol. 68, No. 234/ Friday, December 5, 2003/p. 68140 (68164-5).

<sup>134</sup> It seems that this is a misprint and should read: "shipping companies charge a \$25 fee".

<sup>135</sup> Federal Register/Vol. 68, No. 234/Friday, December 5, 2003/p. 68140 (68165).

### *24-Hour Rule: developments in other jurisdictions*

69. In this context it is important to note that several governments, recognizing the need to enhance trade and transport security worldwide and following the U.S. example, are considering the implementation of similar regulations or legislation. Canada, for instance which for much U.S. bound cargo is a transit country has adopted its own 24-Hour Rule, which will be applicable in relation to all cargo imports as from April 19, 2004.<sup>136</sup> The European Union, too, is actively pursuing a number of different security projects. These include proposals for a regulation, which would introduce, *inter alia*, requirements similar to the U.S. 24-Hour Rule in relation to all EU import and export cargo.<sup>137</sup>

70. These developments are important. They suggest that advance electronic transmission of cargo information for customs purposes may soon become the norm in relation to trade with certain nations and large trading blocks. The above comments are in this respect equally applicable, but an additional concern arises, particularly for smaller developing nations, namely the possibility of a trend towards diverse national regimes, each establishing specific requirements, which need to be complied with by individual traders and carriers.<sup>138</sup> Concerted international efforts towards minimising the potential for different national or regional approaches are, in this context, of particular importance.<sup>139</sup>

---

<sup>136</sup> For more info, see Canada Border Services Agency website at <http://www.cbsa-asfc.gc.ca>.

<sup>137</sup> For further information, see part C.III, below.

<sup>138</sup> For instance, country (A) applies a particular regulation for outbound cargo and country (B) applies another set of rules for inbound cargo. Exporters, importers and carriers involved in trade between these two countries might need to comply with two different sets of rules.

<sup>139</sup> It should be noted that the WCO is working on an integrated Customs control chain, to provide for the collaboration of Customs administrations, see also Part C.I, below.

## C. RELATED INTERNATIONAL DEVELOPMENTS: A BRIEF OVERVIEW

71. International awareness and recognition of the need to enhance maritime transport security has led to a number of important initiatives within different international fora. Thus, the **G8 members** are supporting the development of several security projects and regulations and have agreed a set of co-operative actions to promote greater transport security while facilitating trade<sup>140</sup> and **NATO members** are working on several measures, including measures relevant to maritime and container security.<sup>141</sup> The **European Commission** has begun considering a wide range of relevant initiatives and a number of international organisations, in particular, **ILO**, **WCO** and **IMO** have started devoting their attention to issues relevant to cargo and transport security. While detailed consideration of any of these developments is beyond the scope of this report, the most important relevant developments will be presented in overview.

### I. Developments at the World Custom Organisation

72. Following the implementation of the Container Security Initiative (CSI) in several countries, the World Custom Organisation (WCO) on June 28, 2002, passed a resolution adopting a strategy to safeguard the trade supply chain from terrorist threat and enhance the flow of trade.<sup>142</sup> The resolution called for a number of actions, including

- (i) re-examination of the WCO Data Model "to ensure it includes a standardized set of data elements necessary to identify high-risk goods";
- (ii) the development of "Guidelines to assist Members in developing a legal basis and other necessary steps to enable the advance electronic transmission of Customs data";
- (iii) the development of "Guidelines for cooperative arrangements between Members and private industry to increase supply chain security and facilitate the flow of international trade."

73. An "expert international Task Force" was established to work at standardising information essential to Customs administrations in identifying high-risk cargo while facilitating legitimate trade. One year later, the WCO adopted a series of measures, which had been under discussion within the Task Force.<sup>143</sup> More particularly, the Council approved the following measures:

- A new international Convention and commentary on Mutual Administrative Assistance in Customs Matters;
- The WCO Data Model and a list<sup>144</sup> of essential data elements required for the identification of high risk consignments;
- International Customs guidelines on advance cargo information (ACI Guidelines);

---

<sup>140</sup> For more information on the latest G8 statements on transport security, see [www.g8.fr](http://www.g8.fr).

<sup>141</sup> Among other measures, this includes the "Operation Active Endeavour", which provides for the deployment of NATO naval forces to patrol the eastern Mediterranean and the Strait of Gibraltar and monitor shipping. For more information, see [www.nato.int](http://www.nato.int).

<sup>142</sup> For the full text of the *Resolution of the Customs Co-operation Council on Security and Facilitation of the International Trade Supply Chain*, see the WCO website at <http://www.wcoomd.org>.

<sup>143</sup> For more details, see press release of July 4, 2003 on the WCO website at [www.wcoomd.org](http://www.wcoomd.org)

<sup>144</sup> To access the WCO Data Model and the list of essential data elements, see the relevant links in the press release of July 4, 2003 at <http://www.wcoomd.org>.

- Guidelines for the development of national laws for the collection and transmission of Customs information;
- High level guidelines for co-operative arrangements between WCO Members and the private sector to increase supply chain security;
- Enhancements to the WCO's information and intelligence strategy including the operation of its global RILO (Regional Intelligence Liaison Offices) network;
- A new Internet based technology databank to enable WCO Members to identify technology to assist detection of illegal consignments and contraband.<sup>145</sup>

74. The *International Convention on Mutual Administrative Assistance in Customs Matters* which was adopted on June 27, 2003 provides for Contracting Parties to give each other administrative assistance under the terms of the Convention, "for the proper application of Customs law, for the prevention, investigation and combating of Customs offences and to ensure the security of the international trade supply chain".<sup>146</sup> Administrative assistance may consist in exchanging information on various aspects. For example, Contracting Parties may, by mutual arrangement, "exchange specific information in advance of the arrival of consignments in their respective territories to ensure the security of the international supply chain".<sup>147</sup> Further, assistance may involve Cross-Border Co-operation, where, by mutual arrangement, officials of a Contracting Party engage in activities taking place in the territory of another Contracting Party. They may, *inter alia*, "establish joint control and investigation teams to detect and prevent particular types of Customs offences". Such teams "shall operate in accordance with the law and procedures of the Contracting Party in whose territory the activities are being carried out".<sup>148</sup> Finally, the Convention provides that any information communicated shall be used only by the Customs administration, which requested it and solely for the purpose of administrative assistance under the terms set out in this Convention, any information being treated as confidential and personal data being protected.<sup>149</sup>

75. As for the *International Customs Guidelines on Advance Cargo Information (ACI Guidelines)*, it appears that a final version has not yet been adopted. The latest draft dated May 9, 2003 was presented to the WCO Council in June 2003 where the proposed Guidelines were approved in principle, with a view to finalizing them by the end of 2003. The objective of the proposed Guidelines is for "Customs administrations to develop and agree [bilaterally or multilaterally] on an integrated Customs control chain reaching from origin to destination and addressing the key elements of supply chain security i.e. in document and physical control, shipment personnel and information security".<sup>150</sup> To assist the Customs administrations in that task, the proposed *Guidelines* list and describe various procedures and processes in international trade together with the way they should be included into an integrated Customs control chain. These procedures include the advance electronic transmission of an initial export goods declaration by the exporter or his agent, the advance electronic transmission of an initial declaration by the carrier, the advance electronic transmission of an initial import goods declaration by the importer or his agent and the routine electronic exchange of Customs data between Customs administrations at export and import to support risk assessment and rapid

---

<sup>145</sup> For further information on the individual measures, as well as relevant hyperlinks, see press release of July 4, 2003 ([www.wcoomd.org](http://www.wcoomd.org)).

<sup>146</sup> *International Convention on Mutual Administrative Assistance in Customs Matters*, Art. 2.1.

<sup>147</sup> *Ibid.* Art. 10.1.

<sup>148</sup> *Ibid.* Art. 23.1 and 23.2.

<sup>149</sup> *Ibid.* Art. 24-26.

<sup>150</sup> *Draft ACI Guidelines* (9.5.2003), 1.3.

release.<sup>151</sup> Thus, the *ACI Guidelines* may be seen as an international parallel to the United States' 24-Hour Rule.

76. Countries implementing the *ACI Guidelines* at the national level will have to establish the necessary technical infrastructure, including Customs IT systems, and develop the appropriate legal framework required by their national law. The *ACI Guidelines* will, however, only become effective when Customs administrations will have agreed bilateral or multilateral arrangements and will have implemented the common standards described in the Guidelines.

## II. Developments at the IMO

77. At a diplomatic conference in December 2002, the International Maritime Organisation (IMO) agreed on a new comprehensive security regime for international shipping, by adopting a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS).<sup>152</sup> Chapters V and XI of the Annex to SOLAS were amended, the latter chapter being renumbered as chapter XI-1. Moreover, a new chapter XI-2 on "Special measures to enhance maritime security" was added. That chapter also sets out the new *International Ship and Port Facility Security Code (ISPS Code)*, which applies to all cargo-ships of 500 gross tonnage or above, passenger vessels, mobile offshore drilling units and port facilities serving such ships engaged on international voyages.<sup>153</sup> Part (A) of the Code consists of a list of mandatory requirements and Part (B) provides recommendations on how to fulfil each of the requirements set out in Part (A).

78. The new regime aims at enhancing maritime security on board ships and at the ship/port interface by providing a standardized and consistent framework for the evaluation of risks.<sup>154</sup> The stated main objectives of the ISPS Code are, *inter alia* "to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade" and "to establish the respective roles and responsibilities" of the parties.<sup>155</sup>

79. The new regime is set to enter into force in July 2004 and its timely implementation is mandatory for all 147 SOLAS Member States, without any distinction as to their level of development. Due to its central importance for all involved in maritime transport, the main requirements of the new regime imposed on governments, vessel-owning and/or operating companies, and well as port facilities are here presented in overview.<sup>156</sup>

---

<sup>151</sup> *Draft ACI Guidelines* (9.5.2003), 3.1.3.

<sup>152</sup> See <http://www.imo.org>.

<sup>153</sup> See SOLAS, chapter X-2/2 and ISPS Code (A), Art. 3.

<sup>154</sup> For a good overview, see OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003, p. 28-43; see also Trelawny, *IMO activities to enhance maritime security*, paper presented at the UNCTAD Expert Meeting on the Development of Multimodal Transport and Logistics Services, 24-26 September 2003, available on the UNCTAD website ([www.unctad.org](http://www.unctad.org)); BIMCO Bulletin Vol. 98 – N°3 – 2003.

<sup>155</sup> ISPS Code (A), At. 1.2.

<sup>156</sup> See also O. Özcayir, *The ISPS Code*, *Journal of International Maritime Law* 9 [2003] 578; J. Bruce, *The legal implications of the ISPS Code*, presented at the IIDM Conference in Bariloche, Argentina in October 2003. Copies may be requested from the author ([jonathan.bruce@clyde.co.uk](mailto:jonathan.bruce@clyde.co.uk)).

## 1. Responsibilities of Contracting Governments

80. The principal responsibility of Contracting States under SOLAS chapter XI-2 and Part (A) of the Code is to determine and set security levels (ranging from 1=low to 3=exceptional, imminent risk) and, in cases of security-level 3, to communicate relevant security information to vessels flying their flag, as well as to ports within their territory and foreign flag vessels entering ports within their territory.<sup>157</sup> The alert levels are associated with a number of security measures to be implemented by ship and port operators in order to ensure that security measures correspond to the identified level of risk.

81. Responsibilities also include, among others, the issuance of *International Ship Security Certificates* (ISSC) after *verification*,<sup>158</sup> the approval of *Ship Security Plans*, as well as the carrying out and approval of *Port Facility Security Assessments*, the approval of *Port Facility Security Plans*, the determination of port facilities which need to designate a *Port Facility Security Officer*, and the exercise of *control and compliance measures*.<sup>159</sup>

82. Governments may establish internal Designated Authorities to undertake the relevant security responsibilities and delegate certain responsibilities to Recognized Security Organizations (RSO) outside Government.<sup>160</sup>

## 2. Responsibilities of vessel-owning and/or operating companies

83. A number of responsibilities apply to vessel-owning and/or operating companies, whose principal obligation it is to ensure that each vessel it operates obtains, by July 1, 2004, an *International Ship Security Certificate* (ISSC) from the administration of a flag state or an appropriate RSO, such as a classification society. It has been estimated that more than 43,000 cargo-carrying vessels alone will be affected.<sup>161</sup> Ships, which after July 1, 2004, are found not to be in compliance with the requirements under SOLAS and the ISPS Code face serious repercussions.<sup>162</sup> In order to obtain an ISSC, the following measures must be taken

- **Designation of a Company Security Officer (CSO):** At least one CSO needs to be designated to take ultimate responsibility for company and ship compliance with the new IMO security rules. Detailed duties of the CSO are further specified in the Code, such as co-ordinating Security Assessments, overseeing the development, submission and approval of the Ship Security Plan, liaising with vessels on security issues, maintaining the security system and ensuring the required verifications.<sup>163</sup>
- **Ship Security Assessments (SSA):** Ship owners and operators have to carry out Ship Security Assessments, including an on-site visit for each of their vessels. Assessments are

---

<sup>157</sup> SOLAS, chapter X-2/3; ISPS Code (A), Art. 4 and (B), Art. 4.

<sup>158</sup> ISPS Code (A), Art. 19 and (B), Art. 19.

<sup>159</sup> See ISPS Code (A), Art. 4; SOLAS chapter XI-2/9.

<sup>160</sup> Responsibilities set out in ISPS Code (A), Art. 4.3 may not be delegated to RSOs.

<sup>161</sup> BIMCO Bulletin Vol. 98 – N°3 – 2003; OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003, at p. 28.

<sup>162</sup> See control and compliance measures, part C.II.4, below. Shipowners also face losing the liability cover provided by their Protection and Indemnity (P&I) Clubs, if they fail to obtain the relevant documentation under the ISPS Code, see *Political pressure piles on shipping chiefs to ISPS deadline*, Lloyd's List, 13.1.2004.

<sup>163</sup> ISPS Code (A), Art. 11 and (B), Art. 11.

to be documented, retained and reviewed periodically.<sup>164</sup> The aim of this process is to identify the presence of any existing security measures and assess potential threats and vulnerabilities.

- **Ship Security Plans (SSP):** On the basis of the outcome of the Ship Security Assessment, a Ship Security Plan has to be developed for each vessel. The plan must contain a clear statement emphasising the Master's authority and responsibility in relation to all safety and security matters and identify the Company and Ship Security Officers. The plan should address several issues, such as, among others, measures to prevent unauthorised access, duties of shipboard personnel, responses in cases of threat and safeguards to counter unlawful carriage of weapons. It should also describe specific procedures to deal with given situations, such as reporting incidents, evacuating the ship, inspecting, testing and maintaining the vessel's security equipment or responding to security instructions given by governments.<sup>165</sup> Procedures must also be devised for the reviewing and updating of the plan itself. Completed Ship Security Plans have to be submitted to the flag State administration for approval.
- **Designation of a Ship Security Officer (SSO):** An SSO must be appointed on each ship. His main duties are to implement the Security Plan on board, carry out ship inspections and report incidents. He works in close collaboration with the CSO and Port Security Officers.<sup>166</sup>
- **Training, drills and exercises:** Both CSO and SSO need to be trained, in order to become familiar with the new IMO requirements and their own specific duties. Records must be maintained in that respect. Finally, the crew has to get acquainted with the Ship Security Plan. Security drills are to be held on board at least once every three months to promote the effective implementation of the Ship Security Plan, while a full-scale exercise involving the Company Security Officer has to take place once a year.<sup>167</sup>

### 3. Special provisions applicable to ships

84. A number of special mandatory requirements in SOLAS chapter V, X-1 and X-2 are applicable to ships and create additional responsibilities for vessel-owning companies and for governments.<sup>168</sup>

- **Automatic Identification System (AIS):** The deadline for implementation of mandatory SOLAS requirements to fit merchant vessels with an Automatic Identification Systems (AIS) has been brought forward to 2004.<sup>169</sup> Automatic Identification System are shipboard automatic electronic reporting devices that communicate to other AIS

---

<sup>164</sup> ISPS Code (A), Art. 8 and (B), Art. 8.

<sup>165</sup> ISPS Code (A), Art. 9 and (B), Art. 9.

<sup>166</sup> ISPS Code (A), Art. 12 and (B), Art. 12.

<sup>167</sup> ISPS Code (A), Art. 13 and (B), Art. 13.

<sup>168</sup> SOLAS chapter X-2/4.

<sup>169</sup> SOLAS, chapter V/19. The time-frame for mandatory fitting of ship-borne AIS on all ships of 300 gross tonnage and above, on international voyages, has been brought forward to the first safety equipment survey after 1.7.2004 or to 1.12.2004, whichever occurs earlier.

transponders and shore-based facilities basic information regarding the ship's identity, position, course and speed.<sup>170</sup>

- **Ship Identification Number (SIN):** Vessels need to permanently and prominently display a unique identification number both in a visible place on the outside of the ship and in an easily accessible place in the engine area.<sup>171</sup>
- **Ship Security Alert System (SSAS):** Vessels need to be fitted with a Ship Security Alert System. This system must be capable to be triggered from the bridge and at least one other location to transmit a ship-to-shore security alert.<sup>172</sup>
- **Continuous Synopsis Record (CSR):** As from July 2004, flag State administrations need to issue ships with a Continuous Synopsis Record (CSR) providing information on the ship's name, identification number, flag state, date of registration, port of registry and classification society. The CSR also provides the names and registered address of (a) the registered owner, (b) the bareboat charterer and (c) the "Company" (for the purposes of the ISPS Code), together with the address(es) from where it carries out its safety management activities. Finally, the CSR contains information on the relevant administration or organization, which issued the Company's Document of Compliance, the vessel's Safety Management Certificate and the International Ship Security Certificate.<sup>173</sup> The CSR has to be updated, if necessary, and must be retained on board throughout the entire life of the vessel, irrespective of new management or ownership and must be available for inspection at all times.
- **Record keeping:** Various extensive record keeping requirements apply in relation to ships.<sup>174</sup> In particular, ships shall maintain detailed records of any relevant security information covering at least the last 10 calls at port facilities and must be ready to provide such information.

#### 4. Control and compliance measures

85. As has been mentioned, Contracting States are responsible for control and compliance measures. Vessels inside a foreign port or intending to enter a foreign port are subject to control and need to be able to show that they have a valid *International Ship Security Certificate* as well as relevant security records on board. When no valid ISS Certificate is produced upon request or when there are clear grounds for suspicion that the ship is otherwise not in compliance with SOLAS chapter XI or the ISPS Code, different control and measures may be taken. These range from requests for rectification of non-compliance and the inspection of the ship to its delay, detention, and denial of entry to or expulsion from the port.<sup>175</sup> It should be noted that a ship otherwise compliant with SOLAS chapter XI-2 and part A of the Code may also be subject to

---

<sup>170</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003, p. 30 and <http://www.kleinsonar.com/wss/ais-pdf>.

<sup>171</sup> SOLAS chapter XI-1/3. See also the IMO Maritime Safety Committee (MSC) *Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code*, MSC/Circ.1097, 6.6.2003, at para. 28 ([www.imo.org](http://www.imo.org)).

<sup>172</sup> SOLAS chapter XI-2/6. See also MSC Circulars *Guidance on provision of ship security alert systems* (MSC/Circ.1072) and *Directives for maritime rescue co-ordination centers (MRCCs) on acts of violence on ships* (MSC/Circ. 1073).

<sup>173</sup> SOLAS chapter XI-2/5. See also MSC 77/6/10 for a draft template CSR developed by IMO.

<sup>174</sup> ISPS Code (A), Art. 10 and SOLAS chapter XI-2/9.2.2.

<sup>175</sup> SOLAS chapter XI-2/9.

appropriate control measures if that ship had interactions with a non-compliant port facility or ship.<sup>176</sup>

## 5. Responsibilities of Port Facilities

86. Depending on size, there may be, within the legal and administrative limits of any individual port, several or even a considerable number of port facilities for the purposes of the ISPS Code.<sup>177</sup>

- **Port Facility Security Plans (PFSP):** Based on the Port Facility Security Assessments carried out and - upon completion - approved by the relevant national government,<sup>178</sup> a Security Plan needs to be developed which provides preventive and threats response measures and procedures. The PFSP should, for instance address the question of unauthorized access to the port facility or to ships moored at the facility and the question of evacuation in case of security threats.<sup>179</sup>
- **Port Facility Security Officer (PFSO):** For each port facility, a Security Officer must be designated. Among other duties, the PFSO<sup>180</sup> shall ensure the maintenance and implementation of the Port Facility Security Plan, recommend modifications to respond to the change of circumstances and ensure the appropriate security measures are kept within the facility.
- **Training, drills and exercises:** Port Facility Security Officers as well as port facility security personnel shall receive appropriate training in order to fulfil their duties and responsibilities under the new SOLAS requirements. Regular drills are also required to ensure the effective implementation of the Port Facility Security Plan.<sup>181</sup>

## 6. Implementation, cost implications and potential impacts

87. The wide-ranging nature of the requirements and the tight timeframe for their implementation *by* and *in* all SOLAS Member States has generated understandable concern within the maritime transport and port community,<sup>182</sup> as well as among governments.<sup>183</sup> As recently as January 15, 2004, the IMO has urged SOLAS Contracting States, port authorities,

---

<sup>176</sup> See also proposal for global *Procedures for Port State Security Control*, which has recently been submitted to the IMO Sub-Committee on Flag State Implementation (FSI/12/15), 12.12.2003, at 1.3.6.

<sup>177</sup> See for instance, *Security hot issue in port of Rotterdam*, Port of Rotterdam, Winter 2003, 16, reporting on the development of an ISPS toolkit for use by all terminal operators in Rotterdam's port and industrial area. Reference is made to 140 locations within the area to which the code applies.

<sup>178</sup> ISPS Code (A), Art. 15 and (B), Art. 15.

<sup>179</sup> ISPS Code (A), Art. 16 and (B), Art. 16.

<sup>180</sup> ISPS Code (A), Art. 17 and (B), Art. 17.

<sup>181</sup> ISPS Code (A), Art. 18 and (B), Art. 18.

<sup>182</sup> See for instance, *Will shipping hit ISPS deadline?*, Lloyd's List, 20.8.2003; *Keeping tabs on the maritime enemy; ISPS Code could still cause slips*, Lloyd's List, 21.8.2003; *Managers face tight ISPS deadline*, Fairplay, May 1, 2003; *Port Security still a problem*, Fairplay, May 8, 2003; *Getting ready for the ISPS Code*, Fairplay, August 7, 2003; *Australia row over paying for new rules*, Lloyd's List, 5.2.2004; *Divergence to mark debut of ISPS Code*, Lloyd's List, 4.2.2004.

<sup>183</sup> See MSC Circular *Early implementation of the special measures to enhance maritime security*, MSC/Circ. 1067, 28.2.2003. Member Governments are urged to provide, in co-operation with IMO, assistance to States having implementation difficulties. Those States are encouraged to use the IMO's Integrated Technical Co-operation Programme.

classification societies, recognized security organizations, training institutions and all other parties concerned to redouble their efforts to ensure compliance with the new requirements by the deadline of July 1, 2004.<sup>184</sup> Vessels calling at Paris MOU<sup>185</sup> ports after 1.1.2004 without a valid ISSC are already being issued with a letter of warning by local port state control authorities.<sup>186</sup> The U.S., too, has announced the commencement of pre-enforcement checks as from January 2004 and both the U.S. and Britain have been reported as taking a zero-tolerance approach to enforcement of the ISPS Code.<sup>187</sup>

88. At the same time, recent surveys carried out on the status of implementation of the security measures raise concerns that not enough progress has been achieved so far.<sup>188</sup> This has been reported by governments and other interested parties, including industry organizations, such as the International Chamber of Shipping (ICS), BIMCO, the International Association of Classification Societies (IACS), INTERTANKO, INTERCARGO and the International Association of Ports and Harbours (IAPH).<sup>189</sup>

89. The IAPH survey among its member ports illustrates some of the difficulties.<sup>190</sup> While 70% of the 53 member ports, which responded to the survey, were confident they would meet the deadline of July 1, 2004, 19% were uncertain. Reasons cited for delay in implementations include, above all, financial constraints as well as lack of staff and expertise. Other reasons cited were delay in legislative enactment and procedures by governing bodies and authorities. In particular smaller ports and ports from developing nations called for information sharing and technical assistance, including guidelines, models and samples, as well as financial assistance, such as through the establishment of a funding plan to raise public finance for developing countries. Not surprisingly, ports expressed some concern about a potential increase in security related competition as some countries might impose stricter requirements than others.<sup>191</sup>

---

<sup>184</sup> IMO MSC/Circ. 1104. A detailed proposal for global *Procedures for Port State Security Control* has recently been submitted to the IMO Sub-Committee on Flag State Implementation (FSI/12/15), 12.12.2003.

<sup>185</sup> Paris Memorandum of Understanding on Port State Control.

<sup>186</sup> See announcement of December 16, 2003, <http://www.parismou.org>. Detailed Paris MoU *Draft Guidelines for Port State Control Officers on Security Checks* have recently been submitted by to the IMO Sub-Committee on Flag State Implementation (FSI 12/15/1) 16.12.2003.

<sup>187</sup> See *Zero tolerance as US launches pre-enforcement ISPS checks*, Lloyd's List, 4.2.2004, quoting the head of shipping policy at the British Department of Transport describing the U.S. and British position as one of "zero tolerance".

<sup>188</sup> See *ISPS lag leaves 25,000 ships for auditing in only 210 days*, Lloyd's List, 5.12.2003, where the director of marine business for Lloyd's Register in Asia is reported as suggesting there was a shortage of auditors making it impossible to carry out the required number of audits (120 ships per day) by July 1, 2004; see also *British Companies miss deadline for submitting outline ISPS plans*, Lloyd's List, 4.2.2004.

<sup>189</sup> IMO Press release *Redouble efforts to protect shipping against terrorism, IMO urges* ([www.imo.org](http://www.imo.org)). See also note submitted to IMO Assembly by BIMCO, ICS, INTERCARGO and INTERTANKO on *Progress towards compliance with ISPS Code* (A 23/17/2), 13.11.2003.

<sup>190</sup> See *IAPH Follow-Up Report on Compliance with the Revised SOLAS Convention & ISPS Code conducted in October/November 2003*. The report was submitted to IMO and is available as document MSC 78/INF.3 (17.11.2003). IAPH suggests a scheme to facilitate implementation by ports in need of technical support, with possible assistance of competent ports within the association.

<sup>191</sup> See also note submitted to IMO Assembly by BIMCO, ICS, INTERCARGO and INTERTANKO on *Progress towards compliance with ISPS Code* (A 23/17/2), 13.11.2003, para. 5, noting with concern different requirements regarding training courses.

90. Among shipowners and operators, costs and adequate guidance on the part of flag states appear to be a major concern.<sup>192</sup> According to a recent survey carried out by the Lloyd's Ship Manager (LSM)<sup>193</sup>, over 60% of respondents did not believe that enough adequate information had been made available by flag states regarding the correct course for ISPS preparations and developments. 50% felt that no proper distinction had been made between the security responsibilities of the owner and of the port state control authority. As regards costs, over 60% of respondents considered the ISPS Code as constituting "a major drain" on their budget. More than 70% estimated that the ISPS Code would add an additional \$10,000-\$20,000 to their annual budget per vessel, with 14% estimating their annual costs per vessel to be between \$30,000 and \$40,000. A further 14% envisages annual costs of more than \$50,000 per vessel.

91. It has been reported that flag states are considering charging a fixed fee in the order of US\$ 250 for ISS certificates issued under the ISPS Code.<sup>194</sup> Ports too, have been reported as considering levying security fees of GBP 10.50 or EURO 10 per box.<sup>195</sup> BIMCO has developed a clause for incorporation into time charterparties, which seeks to distribute, as between owners and charterers, the costs of delays and expenses incurred as a result of compliance with the ISPS Code, as well as potential liabilities arising.<sup>196</sup> Under the clause, charterers are responsible for "all delay, costs or expenses whatsoever arising out of or related to security regulations or measures required by the port facility or any relevant authority in accordance with the ISPS Code." Owners are liable for all measures taken to comply with the Ship Security plan and its preparation and must hold a valid International Ship Security Certificate.<sup>197</sup> Again, through incorporation into voyage charterparties and bills of lading, these clauses are likely to affect also shippers and consignees of cargo, i.e. exporters and importers.

92. Some **early OECD estimates on the likely global costs** arising from the new IMO security requirements for ship operators and ports were published in a report issued in July 2003. According to the report, the initial **ISPS Code compliance burden on ship operators** is estimated "to be *at least* ~USD 1 279 million and ~USD 730 million per year thereafter".<sup>198</sup> These estimates relate mainly to management staff and security-related equipment expenditures, but do not include "the costs of implementing IMO AIS requirements (...) and the indirect costs of operating under level 2 and 3 security alerts (potentially very large)".

93. As developing countries, excluding open-registry countries, account for 19 per cent of the world fleet,<sup>199</sup> their set-up costs would, on the basis of these estimates, be about US\$ 250 million and their annual costs about US\$ 140 million. The estimated global freight costs were US\$364 billion in 2001<sup>200</sup> of which about 60 per cent relates to shipping.<sup>201</sup> Thus compliance costs passed

---

<sup>192</sup> For concerns regarding the possible detrimental consequences on national registers arising from the flag state's choice of RSOs, see *Panama under fire again over ISPS strategy*, Lloyd's List, 3.2.2004.

<sup>193</sup> Lloyd's Ship Manager, September 2003, p. 14-15.

<sup>194</sup> *Panama sets \$250 fee target for certificates*, Lloyd's List, 17.7.2003.

<sup>195</sup> See *Group blasts Hutchison fee plan*, South China Morning Post, 13.1.2004. See also *Legal challenge to Hutchison over Felixstowe*, Lloyd's List, 2.2.2004, where it is reported that the legality of these charges in Britain is formally being challenged.

<sup>196</sup> See Annex I. The full text of the clause is available on the BIMCO website at [www.bimco.dk](http://www.bimco.dk). See also *BIMCO clause to clarify ISPS Code cost concerns*, Lloyd's List 3.12.2003.

<sup>197</sup> See further Annex I.

<sup>198</sup> OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 ([www.oecd.org](http://www.oecd.org)), p. 38.

<sup>199</sup> *UNCTAD Review of Maritime Transport 2003*, p. 28, table 13. Percentage refers to 2001. Beginning of 2003, the relevant percentage had risen to 20%.

<sup>200</sup> *UNCTAD Review of Maritime Transport 2003*, p. 73, table 41.

on through an increase in freight to shippers would increase shippers' costs on average by some 0.6 per cent.<sup>202</sup>

94. As concerns the **costs for port facilities**, attempts were made by OECD to quantify different types of direct and indirect costs,<sup>203</sup> and the report concludes that "costs stemming from implementation of the ISPS Code for port facilities are likely to be as large [as those for ship operators], if not larger".<sup>204</sup> OECD has estimated the **global cost of preparing port facility security assessments and plans** to be about US\$ 56 million.<sup>205</sup>

95. Estimating the staff and equipment costs for **implementing the port facility security plan** is, however, extremely difficult given the great variability of needs and costs from port to port.<sup>206</sup> The U.S. Coast Guard had made an estimate of these costs for the United States based on the new investments required to comply with the ISPS Code. They estimated that the initial cost for equipment and guards would be US\$ 907 million with recurring annual costs of US\$ 507 million.<sup>207</sup> This would imply an increase in maritime freight costs of about 4 per cent to cover the set up costs and about 2 per cent thereafter. With the larger number of ports in developing countries (over a hundred countries) and their greater needs, it is likely that their total costs will greatly exceed these figures. The additional investment required in some developing countries would be substantial and immediate.<sup>208</sup> It is estimated that the initial investment needed in developing country ports to implement security plans would be around US\$ 2 billion.<sup>209</sup> Assuming a similar ratio of annual costs to initial costs as estimated by U.S. Coast Guard, the annual cost for developing countries would be US\$ 1 billion.

96. The IMO security requirements place a particularly heavy burden on the poorer developing countries that often lack both the capital and expertise and may face further limitations on their ability to participate in international trade, potentially increasing their existing marginalization.

97. What is critical for developing countries is to assure that their ports or the ports through which they trade are compliant with the ISPS Code. Non-compliance by a port, and it is more likely these will be ports in the LDCs who lack capital and expertise, could lead to ships being unwilling to call. As the vast majority of LDCs trade moves by sea, this could block the trade of

---

<sup>201</sup> Estimate by the UNCTAD secretariat.

<sup>202</sup> Estimated annual compliance costs divided by estimated annual shipping costs (60% of global freight costs).

<sup>203</sup> See OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 (www.oecd.org), p. 39-43.

<sup>204</sup> Ibid., p. 54.

<sup>205</sup> Ibid., p. 40-41.

<sup>206</sup> The port of Rotterdam has developed a Port Facility Security Toolkit, a software tool to enable ports to carry out a risk assessment, generate an Action plan and a detailed Port Facility Security Plan. The toolkit is available free of charge to Dutch ports and port facilities, but foreign ports interested in obtaining the toolkit must pay EURO 40.000, see *Security hot issue in port of Rotterdam*, Port of Rotterdam, Winter 2003,16; *Gaining a competitive edge*, Lloyd's List, Special Issue: The Netherlands, November 2003, 29.

<sup>207</sup> See OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 (www.oecd.org), p. 43. Figures here referred to exclude estimated costs for Port Facility Security Assessments and PFS Plans.

<sup>208</sup> See e.g. concerns of Caribbean countries, reported in Lloyd's List 30.1.2004 (*Caribbean fears US trade link loss*).

<sup>209</sup> This is based on an U.S. Coast Guard estimate of US\$ 441 million for security equipment in U.S. ports (86 ports listed in AAPA Directory and probably at least 5-6 facilities per port). There are over 5,600 port facilities in the world. Assuming half of these facilities are in developing countries and investments required are a minimum of \$500,000 per facility, a minimum global cost estimate is US\$ 1.4 billion and applying a safety factor of 50 per cent a reasonable estimate of the cost would be US\$ 2 billion.

both their imports and exports. As this would be catastrophic on both the humanitarian and economic level, it may be that international action would be taken where certain shipping lines would be granted exceptions to allow them to call while steps are taken to achieve compliance. The magnitude of this problem will become evident in due course.

## 7. Related developments

98. Based on a resolution adopted by the 2002 SOLAS Conference, IMO and ILO have addressed two further aspects relevant to maritime security.<sup>210</sup>

99. In relation to **security in port areas**, a joint draft *IMO/ILO Code of Practice on Security in Ports* has recently been developed.<sup>211</sup> The Code of Practice is intended to complement the provisions of the ISPS Code on port facilities by extending considerations of security to the wider port area. It is expected that the Code of Practice will be approved in the spring of 2004.

100. In relation to **seafarers' identity documents**, the ILO, at its 91<sup>st</sup> session in June 2003 adopted the *Seafarers' Identity Documents Convention (Revised)*, 2003 (No. 185). The Convention provides for a uniform and global identity document that will permit the positive verifiable identification of the world's 1.2 million seafarers. The Convention creates a more rigorous identity regime for seafarers, and sets out the basic parameters with details in annexes for the precise form of the document, including a biometric template based on a fingerprint.<sup>212</sup> It requires each commercial seaman in international trade to carry a biometric ID card based on a fingerprint template encoded in bar code, conforming to a standard to be developed.

## III. European Union Developments

101. In July 2003, the European Commission made several proposals to amend the *Community Customs Code* in order to simplify administration and strengthen security at its external borders.<sup>213</sup> Among other measures aiming at tightening security around goods crossing international borders, one concerns the introduction in Europe of customs requirements similar to the U.S. 24-Hour Rule, but allowing for risk assessment of cargo in-transit, rather than pre-loading. It provides for cargo information to be electronically submitted to Customs 24 hours before they are imported into or exported from the European Union. This proposal is currently under review.<sup>214</sup>

---

<sup>210</sup> Resolution 8, adopted at the IMO Conference on December 12, 2002 provides a mandate for co-operation between IMO and ILO on seafarers' identity documents and further work on the wider issue of port security, see [www.imo.org](http://www.imo.org).

<sup>211</sup> A copy of the *IMO/ILO Draft Code of Practice on Security in Ports* as revised by a Sub-Committee of the Tripartite Meeting of Experts on Security, Safety and Health in Ports, held in Geneva in December 2003, is available on the IMO website, [www.imo.org](http://www.imo.org).

<sup>212</sup> See [www.ilo.org/ilolex/cgi-lex/convde.pl?C185](http://www.ilo.org/ilolex/cgi-lex/convde.pl?C185) for the text of the Convention.

<sup>213</sup> See "Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee: a simple and paperless environment for Customs and Trade; Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee on the role of customs in the integrated management of external borders, *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EEC) N° 2913/92 establishing the Community Customs Code*" [COM(2003) 452 final; 2003/0167 (COD)]; see also Press release IP/03/1100 on the European Commission website [http://www.europa.eu.int/comm/taxation\\_customs/customs/customs.htm](http://www.europa.eu.int/comm/taxation_customs/customs/customs.htm).

<sup>214</sup> The decision making process may be followed by consulting the European Commission website. See also the *Council Resolution of 5 December 2003 on creating a simple and paperless environment for customs and trade*, OJ C 305/1, 16.12.2003.

102. Another initiative worth noting, although not specifically related to container security, is the proposal made by the Commission to adopt a *Regulation on enhancing ship and port facility security*.<sup>215</sup> The main objective of the proposed Regulation is to "introduce and implement Community measures aiming at enhancing the security of ships used in international trade and domestic shipping and associated port facilities in the face of threats of intentional unlawful acts". The proposed Regulation also intends to ensure the harmonised interpretation, implementation and monitoring throughout the European Union of the security standards adopted by the IMO. It provides for the mandatory application in full of the measures on maritime security defined in the SOLAS Convention and in Part A of the ISPS Code. The proposed Regulation goes, however, beyond the measures adopted under the auspices of IMO. For instance, it makes mandatory some requirements that are only recommendations under the IMO framework. Also, it extends specific requirements to other vessel types than those provided for in the IMO measures.<sup>216</sup>

#### IV. Developments at the OECD

103. Mention should also be made of work on maritime transport security issues carried out by the Organisation for Economic Cooperation and Development (OECD), through its Maritime Transport Committee.<sup>217</sup> The stated objective of the Committee's efforts is to assist in "establishing a secure transport network without seriously hindering the flow of trade and people or placing unnecessary burdens on governments and industry".<sup>218</sup> The Committee intends to provide its own input to policy debate on current issues.

104. As has already been mentioned, a report on "*Security in Maritime Transport: Risk Factors and Economic Impact*" was published in July 2003.<sup>219</sup> The goal of the study was to examine, in a first stage, the different types of risks faced by the transport network in order to establish, in a second stage, when and how to apply security measures. Existing and proposed international security measures were examined, the level of costs imposed by these measures identified and the distribution of those costs among the different actors of the maritime transport chain evaluated.

105. Estimates provided in the report as to the likely costs associated with some of the relevant U.S. security measures discussed above, as well as with compliance with the new IMO security requirements have already been referred to in the relevant context earlier in this report.<sup>220</sup>

106. Another relevant OECD project, conducted in cooperation with the European Conference of Ministers of Transport (ECMT) and the Road Transport Research Programme of OECD, is

---

<sup>215</sup> See "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on enhancing maritime transport security, *Proposal for a regulation of the European Parliament and of the Council on enhancing ship and port facility security*", [COM (2003) 229 final; 2003/0089 (COD)]

<sup>216</sup> See also *Fight against terrorism: Security of European maritime transport to be strengthened*, Commission Press Release IP/03/651 at <http://www.europa.eu.int>.

<sup>217</sup> Four projects are being developed by the Committee: "Ownership and control of ships", "Risk Analysis and Economic Implications", "Verification of cargoes" and "Best practices guides on security related activities". For more information, see <http://www.oecd.org>.

<sup>218</sup> [http://www.oecd.org/document/53/0,2340,en\\_2649\\_34367\\_2088757\\_1\\_1\\_1\\_37433,00.html](http://www.oecd.org/document/53/0,2340,en_2649_34367_2088757_1_1_1_37433,00.html)

<sup>219</sup> A copy of the report is available at <http://www.oecd.org>. See also *OECD targets terrorism and substandard shipping*, Lloyd's List, 9.6.2003.

<sup>220</sup> See paras. 55, 66, 92 *et. seq.*, above.

called "Verification of cargoes".<sup>221</sup> The project aims at investigating strategies to better ensure the integrity of containerised cargoes in particular by evaluating technical options, cargo processing practices and cost burdens along container transport chains.

107. Finally, mention should be made of efforts to develop *Best practices guides on security related activities*. This activity "attempts to pull together various 'best practices' for a range of transport security responses to provide national administrations and industry bodies with readily available information to take into account when assessing their security needs."<sup>222</sup>

---

<sup>221</sup> See *Maritime Transport Committee Annual Report 2002*, at <http://www.oecd.org>.

<sup>222</sup> *Ibid.*

## D. CONCLUDING REMARKS

108. As has become evident, a variety of different unilateral and multilateral security measures regulations and legislative initiatives have been developed or are under consideration. These impose diverse and wide-ranging requirements on all actors involved in international maritime transport.

109. While there is universal agreement on the need to enhance maritime transport security, it is clear that security requirements may have serious impacts. Concerns, particularly for developing countries, fall broadly into four categories, namely

- Costs and expenses, both direct and indirect;
- Delays and disruption of legitimate trade;
- Difficulty in the implementation of diverse and detailed requirements, due to lack of technical infrastructure, expertise and know-how;
- Competitive imbalances and marginalization resulting from the above.

110. As has been pointed out by the OECD report, in 2002,<sup>223</sup> security measures may have a significant impact on trade flows. "Elasticity of trade flows with respect to transaction costs are estimated to range between -2 and -3, implying that even a relatively small increase in the costs of trading internationally in the order of 1 per cent would lead to a drop in trade flows of between 2 and 3 per cent".<sup>224</sup> "The effect of the proposed tightening of security on the cost of trading internationally is likely to be asymmetrical. Developing country exports often have higher *ad valorem* transportation costs (...) and should thus be affected disproportionately. A "certification" procedure with selected foreign ports could be discriminatory if developing country ports fail to qualify. "Know-your-partner" initiatives, whereby pre-registered intermediaries go through simplified border procedures, may also favour large trading companies over smaller developing country-based firms. These proposed measures risk creating a "slow lane" for developing country exports, increasing relative compliance costs and eroding their competitiveness".<sup>225</sup>

111. There is general consensus on the need for enhancement of maritime and transport security. However, there is also consensus that measures should be internationally uniform<sup>226</sup> and be developed in international co-operation, that they should be based on risk-assessment, be proportionate and balanced and should disrupt legitimate trade as little as possible.<sup>227</sup> Finally, there is consensus that security measures should not serve as a pretext for protectionism and

---

<sup>223</sup> OECD Economics Department Working Paper No. 334, *The economic consequences of terrorism* (ECO/WKP(2002)20), 17.7.2002 (<http://www.oecd.org/eco>). Also published in *Ports and Harbours* (2002).

<sup>224</sup> *Ibid.* at para. 32.

<sup>225</sup> *Ibid.* at page 28 (Box 8, The impact on developing countries).

<sup>226</sup> See on this issue for instance D. Stasinopoulos, *Maritime Security – The Need for a Global Agreement*, *Maritime Economics & Logistics*, 2003, 5 (311-320).

<sup>227</sup> See a recent UN General Assembly Resolution: "Recognizing that countries take appropriate and necessary security measures, but also *underlining* the importance of these being taken in a manner that is least disruptive of normal trade and related practices" (A/C.2/58/L.32 at X).

create unnecessary barriers to trade.<sup>228</sup> While some efforts have already been made to analyse security related costs and their impacts<sup>229</sup>, as well as possible international strategies<sup>230</sup>, much more work is required in this respect.

112. A good summary of relevant considerations, which appear to be shared widely among both public and private parties<sup>231</sup>, may be found in statements made by the European Economic and Social Committee in 2002.<sup>232</sup>

"Security is an issue where all links in the transport chain should be involved and through the door-to-door concept all modes of transport are affected by security considerations at varying degrees. Hence an interoperability of the logistical chain is required".<sup>233</sup>

"The cost and the distribution of cost of security measures should be based on estimates of reasonable measures that could be put in place in order to prevent or reduce the risk of terrorist attacks. The analysis should measure the actual cost of implementation, direct and indirect costs to transport providers and shippers (e.g. delays and additional equipment), impact on world trade and distortions on trading patterns (by trade being redirected to areas of lesser security)".<sup>234</sup>

"Unavoidably, the enhancement of security will involve costly arrangements in terms of hardware (infrastructure and equipment) and software (manpower and training). Care should be taken to avoid disproportionate technical arrangements which may be seen as protectionist and promoting commercial interests. Furthermore the scope and level of measures should take into account any adverse implications on the performance of the human element (...)".<sup>235</sup>

"New security measures should be balanced in relation to the objectives they pursue, their costs and impact on traffic (...)". "New technical norms should not be introduced under the guise of increased security whilst in fact serving other purposes (e.g. commercial promotion of new equipment, protectionism)".<sup>236</sup>

---

<sup>228</sup> See for instance Advance Written Questions on the WTO's *Trade Policy Review United States*, available as part of the relevant documentation on the discussions which took place on 14 and 16 January 2004 on the WTO website ([www.wto.org](http://www.wto.org)).

<sup>229</sup> See e.g. OECD Report *Security in Maritime Transport: Risk Factors and Economic Impact*, July 2003 ([www.oecd.org](http://www.oecd.org)); WCO commissioned study, P. Dulbecco and B. Laporte, *How can the security of the international supply chain be financed?*, April 2003, [www.wcoomd.org](http://www.wcoomd.org).

<sup>230</sup> For instance, Netherlands Customs has prepared a discussion document for consideration within WCO, *Supply chain security: where do we want to go?*

<sup>231</sup> See also comments on maritime security made by the President and CEO of the World Shipping Council in his testimony to the U.S. House Transportation and Infrastructure Committee in March 2002: "First, there must be a unified, coordinated strategy to address this issue. (...) Second, there should be clear, mandatory rules informing each responsible person in the transportation chain what is required of them. (...) Third, the security regime must allow for the continued free and efficient flow of trade. (...) Fourth, international cooperation is necessary to effectively and comprehensively extend enhanced security to international supply chains". See <http://www.house.gov/transportation/cgmt/03-13-02/koch.html>.

<sup>232</sup> See *Opinion of the European Economic and Social Committee on the 'Security of Transports'* (2003/C61/28), Official Journal (OJ) C 61/174, 14.3.2003, available at <http://europa.eu.int/eur-lex>.

<sup>233</sup> Ibid., para. 7.6.

<sup>234</sup> Ibid., para. 2.4.1.

<sup>235</sup> Ibid., para. 2.4.5.

<sup>236</sup> Ibid., para. 7.11.

"Given the international character of maritime and air transport, security requirements should be based on reciprocal arrangements, uniformly applied and enforced without discrimination and must allow for the most efficient flow of trade". (...) "There is a need to coordinate the decision-making processes in international fora and at the EU level in order to avoid possible inconsistencies (...). Unilateral and arbitrary measures should be avoided since they hamper world trade by raising bureaucratic as well as other obstacles, and eventually leading to distortions of competition and adverse economic effects".<sup>237</sup>

113. In view of the fact that transport security measures are going to form an integral part of the international trading environment, it is important that considerations such as the above are taken into account in any further discussions on the subject. In this context, particular attention may need to be paid to the position of developing countries.

---

<sup>237</sup> Ibid., para. 7.5 and 7.7.

## Annex I

### New standard term contract clauses developed by BIMCO

1. The various clauses are here presented in overview only. For the full text of all clauses, see the BIMCO website at <http://www.bimco.dk>

#### U.S. C-TPAT Clause

2. This clause has been drafted to take account of the situation where the charterers of a vessel have voluntarily signed the C-TPAT Agreement, but the owners have not.

3. The clause states that *"the Owners, Master and Crew will use reasonable efforts to assist the Charterers to comply with their obligations under the C-TPAT Agreement. However, under no circumstances shall the Owners, Master and Crew be liable for any delays, losses or damages howsoever arising out of any failure to meet the requirements of the C-TPAT Agreement signed by the Charterers"*.

4. Further the clause provides that *"the Charterers agree to indemnify and hold the Owners, Master and Crew harmless for any claims made against the Owners, Master and Crew or for any delays, losses, damages, expenses or penalties suffered by the Owners arising out of the C-TPAT Agreement signed by the Charterers"*.

5. According to this clause, shipowners undertake to assist charterers to comply with their obligations under the C-TPAT Agreement, without, however, incurring any legal obligation. The clause ensures that the non-contractual C-TPAT agreement entered into by a charterer does not create any legally binding obligation on the part of a shipowner.

#### U.S. Security Clauses

6. Two clauses, one for use in voyage charterparties and one for use in time charterparties, have been drafted to establish, as between charterers and owners, liability for time lost and expenses incurred as a consequence of any U.S. security regulations or measures. This includes for instance liability arising out of new reporting procedures or the posting of security guards on board vessels calling at U.S. ports.

7. Under a **voyage charterparty**, the owners usually need to comply with and pay for port related requirements and costs. However, as some aspects of the new U.S. security initiatives may give rise to costs, which are exclusively cargo related, the clause provides for these costs to be for the charterer's account. Thus, the clause states that *"if the vessel calls in the United States" and "with respect to any applicable security regulations or measures", "any expenses or additional fees relating to the cargo, even if levied against the Vessel, that arise out of security measures imposed at the loading and/or discharging port and/or any other port to which the Charterers order the Vessel, shall be for the Charterers' account"*.

8. Moreover, while under a voyage charterparty tender of a notice of readiness to load is normally only effective if the vessel is physically and legally ready to receive the cargo, the clause also provides that notice of readiness for loading may be tendered even when the vessel has not been cleared for entry by the authorities. Indeed, the clause provides that *"notwithstanding anything to the contrary contained in this Charter Party the Vessel shall be*

*entitled to tender Notice of Readiness whether cleared for entry or not by any relevant U.S. authority".*

9. The purpose of this part of the clause is to protect the owners against claims by the charterers that the vessel is not legally ready although she is ready for all other purposes. As a consequence, the costs associated with any ensuing delay in loading would be borne by the charterers, not the shipowners.

10. Under a **time charterparty**, the employment i.e. use of the vessel is, within the contractually agreed trading limits, solely the charterer's prerogative. Thus, the new clause for use in time charterparties simply provides explicitly for all costs and expenses arising from security regulations or measures to be for the charterer's account.

11. The clause states that *"if the vessel calls in the United States" and "with respect to any applicable security regulations or measures", "notwithstanding anything else contained in this Charter Party all costs or expenses arising out of or related to security regulations or measures required by any U.S. authority including, but not limited to, security guards, launch services, tug escorts, port security fees or taxes and inspections, shall be for the Charterers' account, unless such costs or expenses result solely from the Owners' negligence"*.

#### U.S. Customs 24-Hour Rule Clauses

12. As mentioned above<sup>238</sup>, failure to comply with the 24-Hour Rule may result in refusal or delay in the issue of a permit to discharge the cargo in the U.S. and/or the assessment of penalties or claims for liquidated damages levied on the carrier by U.S. Customs. However, based on the assumption that charterers are usually in a better position than shipowners to obtain and assess the correctness of cargo-related information, two standard clauses have been drafted to effectively protect shipowners operating under time and voyage charterparties. Both clauses lay down the general principle that charterers have to provide the owners with all necessary cargo information to enable them to submit a timely and accurate cargo declaration. However, where U.S. Customs regulations permit, charterers must submit cargo declarations directly to U.S. Customs.

13. Pursuant to sub-clauses (a)(i) and (ii) of both clauses, *"if loading cargo destined for the US or passing through US ports in transit, the Charterers shall provide all necessary information, upon request by the Owners, to the Owners and/or their agents to enable them to submit a timely and accurate cargo declaration directly to the U.S. Customs; or if permitted by U.S. Customs Regulations (19 CFR 4.7) or any subsequent amendments thereto, submit a cargo declaration directly to the US Customs and provide the Owners with a copy thereof"*. Further, sub-clause (b) of both clauses deals with liability and provides that *"the Charterers assume liability for and shall indemnify, defend and hold harmless the Owners against any loss and/or damage whatsoever (including consequential loss and/or damage) and any expenses, fines, penalties and all other claims of whatsoever nature, including but not limited to legal costs, arising from the Charterers' failure to comply with the provisions of subclause (a)"*.

14. Finally, sub-clause (c) deals with detention, seizure or any other similar situations due to the charterers' failure to comply with the requirements of sub-clause (a) and with the consequences of the time lost. In both clauses, sub-clause (c) states that *"if the vessel is detained,*

---

<sup>238</sup> See part B.I.3.

*attached, seized or arrested as a result of the Charterers' failure to comply with the provisions of sub-clause (a), the Charterers shall provide a bond or other security to ensure the prompt release of the Vessel". The provision further deals with the consequences of the time lost because of detainment, seizure or other similar situation. As far as voyage charterparties are concerned, the relevant clause provides that "all time used or lost until the Vessel is free to leave any port of call shall count as laytime or, if the Vessel is already on demurrage, time on demurrage". As for time charterparties, the relevant clause provides that, "notwithstanding any other provision in this Charter Party to the contrary, the Vessel shall remain on hire".*

#### U.S. trade - unique bill of lading identifier clause

15. The clause provides that *"Charterers warrant that each transport document accompanying a shipment of cargo destined to a port or place in the United States of America shall have been endorsed with a Unique Bill of Lading Identifier as required by the U.S. Customs Regulations (19 CFR Part 4 Section 4.7.a) including subsequent changes, amendments or modifications thereto, not later than the first port of call."*

16. Failure to comply with this provision *"shall amount to breach of warranty for the consequences of which the Charterers shall be liable and shall hold the Owners harmless and shall keep them indemnified against all claims whatsoever which may arise and be made against them."* Moreover, all time lost and all expenses and fines incurred as a result of breach of the provision are to be for the charterers' account.

#### ISPS Clause for Time Charter Parties

17. This clause deals with the distribution of the costs of compliance with SOLAS and ISPS Code security requirements and addresses responsibility for delay, expenses and liabilities arising from non-compliance. The clause also provides for charterer and owner to provide each other with relevant documentation.

18. Sub-clause (a) establishes the owners' obligation to ensure compliance with all SOLAS and ISPS vessel and company requirements and, upon request, to issue charterers with a copy of a valid International Ship Security Certificate (ISSC), as well as the Company Security Officer's contact details. Further, unless otherwise provided elsewhere, all responsibility for *"loss, damage, expense or delay, excluding consequential loss, caused by failure on the part of the Owners or "the Company" to comply with the requirements of the ISPS Code or this Clause shall be for the Owners' account."*

19. Under sub-clause (b), charterers *"shall provide the CSO and the Ship Security Officer (SSO)/Master with their full style contact details and, (...) ensure that the contact details of all sub-charterers are likewise provided to the CSO and the SSO/Master."* Furthermore, the provision requires Charterers to ensure that all sub-charterparties contain a relevant clause. Unless otherwise provided in the charterparty, responsibility for *"loss, damage, expense or delay, excluding consequential loss, caused by failure on the part of the Charterers to comply with this Clause shall be for the Charterers' account"*.

20. Sub-clause (c) allocates responsibility for *"all delay, costs or expenses whatsoever arising out of or related to security regulations or measures required by the port facility or any relevant authority in accordance with the ISPS Code including, but not limited to, security guards, launch services, tug escorts, port security fees or taxes and inspections"* to Charterers, *"unless such costs*

*or expenses result solely from the Owners' negligence". The Owners shall be responsible for "all measures required by the Owners to comply with the Ship Security Plan".*

21. Finally, under sub-clause (d), the parties agree to indemnify each other in respect of any payments made in respect of the other party's responsibilities.

## ANNEX II

### *ABBREVIATIONS*

AAPA	American Association of Port Authorities
ACI	Advance Cargo Information
AIS	Automatic Identification System
AMS	Automated Manifest System
APL	American President Lines
BIMCO	Baltic and International Maritime Council
CBP	U.S. Bureau of Customs and Border Protection
CFR	U.S. Code of Federal Regulations
CMA CGM	Compagnie Maritime d'Affrètement, Compagnie Générale Maritime
COSCO	China Ocean Shipping Companies Group
CSCL	China Shipping Container Line
CSI	Container Security Initiative
CSO	Company Security Officer
CSR	Continuous Synopsis Record
C-TPAT	Customs Trade Partnership Against Terrorism
ECMT	European Conference of Ministers of Transport
ESC	European Shippers' Council
EU	European Union
FAK	Freight of All Kinds
FDA	U.S. Food and Drug Administration
FMC	U.S. Federal Maritime Commission
FROB	Foreign Cargo Remaining on Board
FSI	Flag State Implementation
GAO	United States General Accounting Office
HMM	Hyundai Merchant Marine
HTSUS	Harmonized Tariff Schedule of the United States
IACS	International Association of Classification Societies
IAPH	International Association of Ports and Harbours
ICS	International Chamber of Shipping
IIDM	Iberoamerican Institute of Maritime Law
ILO	International Labour Organization
IMO	International Maritime Organization
INTERCARGO	International Association of Dry Cargo Ship Owners
INTERTANKO	International Association of Independent Tanker Owners
ISPS	International Ship and Port Facility Security
ISSC	International Ship Security Certificate
LCL	Less Than a Container Load
LDCs	Least Developed Countries
LSM	Lloyd's Ship Manager
MOL	Mitsui OSK Lines
MOU	Memorandum of Understanding
MSC	Maritime Safety Committee
MTSA	Maritime Transportation Security Act
NATO	North Atlantic Treaty Organization
NVOCC	Non-Vessel Operating Common Carrier

NYK	Nippon Yusen Kaisha
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal
OOCL	Orient Overseas Container Line
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
P&I	Protection and Indemnity
RILO	Regional Intelligence Liaison Offices
RSO	Recognized Security Organizations
SIN	Ship Identification Number
SOLAS	Safety of Life at Sea Convention
SSA	Ship Security Assessment
SSAS	Ship Security Alert System
SSO	Ship Security Officer
SSP	Ship Security Plan
STC	Said To Contain
TEU	Twenty-Foot Equivalent Unit
UNCTAD	United Nations Conference on Trade and Development
US	United States of America
USC	United States Code
USCS	U.S. Customs Service
WCO	World Customs Organization
WMD	Weapons of Mass Destruction
WSC	World Shipping Council
WTO	World Trade Organization