

LEGISLATION DRAFTING PROJECT

A Legislation Drafting Project Submitted to the International Maritime Law Institute (International Maritime Organisation) in Partial Fulfillment of the Requirements for the Award of the Degree of Master of Laws (LL.M.)

MARITIME SECURITY PACKAGE

Set of Legislation and Sub-legislative Acts for the
Implementation of the IMO Maritime Security Standards set
out in the

SUA Convention and Protocol 1988,

**Chapter XI of the SOLAS Convention 1974 as amended
2002**

and the
ISPS Code

into the
Croatian Legal System

by
Adriana Vincenca Padovan
Croatia

Mentor: Mr. Norman Martinez
Academic Year: 2002-2003



International Maritime Law Institute
MALTA, April 2003

I. SUA 1988

**INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF
UNLAWFUL ACTS AGAINST THE SAFETY OF MARITIME
NAVIGATION, 1988
AND THE
PROTOCOL FOR THE SUPPRESSION OF UNLAWFUL ACTS
AGAINST THE SAFETY OF FIXED PLATFORMS LOCATED ON
THE CONTINENTAL SHELF, 1988**

**- Act of Ratification -
- Announcement of Entry into Force -**

II. THE CRIMINAL LAW OF THE REPUBLIC OF CROATIA

- The Law on the Amendments to the Criminal Law -

III. SOLAS - CHAPTER XI & ISPS CODE

**AMENDMENTS TO THE ANNEX TO THE 1974 CONVENTION
FOR THE SAFETY OF LIFE AT SEA OF DECEMBER 2002
AND THE
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND
OF PORT FACILITIES (ISPS CODE)**

- Decree to Publish the Amendments -**
- Publication of the ISPS Code -**
- Announcement of Entry into Force -**

TABLE OF CONTENTS

▪ Explanatory Note	1
I. SUA Convention and Protocol, 1988	
▪ <i>Act of Ratification</i> of the Convention for the Suppression of the Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf	24
▪ <i>Announcement of entry into force</i>	41
II. The Criminal Law of the Republic of Croatia	
▪ <i>The Law on the Amendments to the Criminal Law of the Republic of Croatia</i>	42
III. SOLAS 1974 Chapter XI & ISPS Code	
▪ <i>Decree to Publish</i> the Amendments (December 2002) to the Annex to the 1974 Convention for the Safety of Life at Sea	45
▪ <i>Publication</i> of the ISPS Code	63
▪ <i>Announcement of entry into force</i>	168

EXPLANATORY NOTE

A. Background

In the light of the unfortunate events of September 11th 2001 and of the growing danger of international terrorism, the Republic of Croatia recognises the importance of global fight against this problem. Over the past couple of years, Croatia has particularly supported all the international efforts of suppressing international terrorist acts and has become a party to the 1977 European Convention on the Suppression of Terrorism and to a number of bilateral treaties on the suppression of terrorism. Croatia is also a party to the international conventions dealing with the suppression of terrorism in Civil Aviation. However, Croatia has never ratified the 1988 SUA Convention and the Protocol thereto¹, even though it has implemented its ideas partly in the domestic legal system, but probably more modelled on the corresponding aviation conventions.

Today, when the matters of security gain the utmost importance, and bearing in mind Croatia's orientation towards the sea and maritime commerce, it is mandatory that the Republic of Croatia ratify the 1988 SUA Convention and Protocol and harmonize its domestic laws to better implement these instruments and to provide for legal security. Moreover, it is urged that the new developments in the international maritime security law be taken into account, particularly the amendments to the SOLAS Convention that introduce a wholly new chapter XI and an International Code for the Security of Ships and of Port Facilities (ISPS Code). These amendments to SOLAS were adopted at the Diplomatic Conference held in London in December 2002 within the International Maritime Organisation (IMO). Otherwise, Croatia would undoubtedly be excluded from the international maritime trade. For all these reasons, adoption of a complete maritime security package of measures is proposed.

SUA Convention & Protocol, 1988

The history of these two international instruments began during the 1980s when the concern about ever more frequent unlawful acts threatening the safety of ships and the security of their passengers and crews started growing. The first action was taken pursuant to the *Achille Lauro* incident in 1983. In November 1985 the problem was considered by the IMO 14th Assembly when a proposal by the United States to develop measures to prevent such unlawful acts was supported. The idea was to provide for measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers, taking into account different incidents, such as piracy, seizure and hijacking, armed robbery and other unlawful acts against or on board ships, including small craft, both at anchor and under way. The task was entrusted to the Maritime Safety Committee. The measures were to take into account the work of the International

¹ Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, Rome 1988

Civil Aviation Organization (ICAO) in the development of standards and recommended practices for airport and aircraft security. Finally, in November 1986 the Governments of Austria, Egypt and Italy proposed that IMO prepare a convention on the subject of unlawful acts against the safety of maritime navigation. The proposal was supported, and in March 1988 a conference was held in Rome which adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.²

The main purpose of the convention is to ensure that appropriate action is taken against persons committing unlawful acts against ships. The Protocol extends the application of the Convention to the fixed platforms located on the Continental Shelf. These include the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. The Convention obliges the States Parties either to extradite or prosecute alleged offenders.

In the light of new unfortunate development and a new era of terrorist attacks, the Legal Committee is reviewing the SUA Convention and its related Protocol. The amendments were expected at the IMO Diplomatic Conference held in December 2002, but this Conference only adopted the amendments to Chapter XI of the Annex to SOLAS including the ISPS Code.

SOLAS - Chapter XI and ISPS Code

The Conference, held at the London headquarters of the International Maritime Organization (IMO) from 9 to 13 December adopted a new, comprehensive security regime for international shipping which is set to enter into force in July 2004. The Conference adopted a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS), the most far-reaching of which are the new Chapter XI of the Annex to SOLAS and the International Ship and Port Facility Security Code (ISPS Code) that is an integrated part of the Convention. The Code contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B).

The purpose of the Code is to provide a standardized, consistent framework for evaluating risk. At the beginning of the process, all States Parties will conduct port facility security assessments. In doing so, they will identify and evaluate important assets and infrastructures critical to the port facility and those areas or structures that, if damaged, could cause significant loss of life or damage to the port facility's economy or environment. Furthermore, they will determine the actual threats to those critical assets and infrastructures, weaknesses of their port facilities in physical security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, and other areas within a port facility that may be a likely target.

² www.imo.org

The Code sets out a number of minimum functional security requirements for ships and port facilities. For ships, these requirements will include ship security plans, ship security officers, company security officers and certain onboard equipment. For port facilities, the requirements will include port facility security plans, port facility security officers and certain security equipment. In addition the requirements for ships and for port facilities include monitoring and controlling access, monitoring the activities of people and cargo and ensuring security communications are readily available.

Ships will be subject to a system of survey, verification, certification, and control to ensure that their security measures are implemented. Port facilities will also be required to report certain security related information to the Contracting Government concerned, which in turn will submit a list of approved port facility security plans, including location and contact details to IMO. Ships will have to carry an International Ship Security Certificate indicating that they comply with the requirements of SOLAS chapter XI-2 and part A of the ISPS Code. When a ship is at a port or is proceeding to a port of a State Party, the State Party has the right to exercise various control and compliance measures with respect to that ship. The ship is subject to port State control inspections but such inspections will not normally extend to examination of the Ship Security Plan itself except in specific circumstances.

To conclude, the amendments will enter into force following the tacit amendment procedure, and Croatia being party to the SOLAS Convention will therefore be obliged to comply with these amendments. All instances of maritime administration and the shipping companies have a huge task to undertake and measures to be able to comply with the new standards. The process needs to begin as soon as possible, since the deadline is July 2004.

B. Harmonisation of the Domestic Legislation with the International Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 1988 (SUA Convention and Protocol)

The incorporation of SUA Convention and Protocol, according to Croatian law is done through the ratification by the Parliament and due publication in the official gazette – “Narodne Novine”. The Convention thereby becomes a part of domestic law and by its legal force it is above the national laws³, which means that if a provision of the Convention and a provision of a national law were to be inconsistent, the Convention would prevail. Furthermore, article 5 of the Convention imposes an obligation on the State Parties to make the offences set forth in the Convention punishable, taking into account the grave nature of those offences. This is to be done through qualification of these offences in a national legislative act which would also prescribe the appropriate punishments. Following the logics of the Croatian legislative system and the fact that the offences of such nature are codified in the Criminal Law of the country, the Criminal

³ Art. 140. of the Constitution of the Republic of Croatia.

Law needs to be amended to accommodate the requirements of SUA Convention and Protocol. Finally, for the purpose of legal certainty, it is advisable to have national laws harmonized with the international conventions. Therefore, as a part of incorporation of SUA Convention and Protocol into Croatian legal system, certain amendments to the Criminal Law are being proposed.

1. OBJECTS OF APPLICATION

SUA Convention & Protocol	The Criminal Law
<p>Convention: Article 1</p> <p>For the purposes of this Convention, "ship" means a vessel of any type whatsoever not permanently attached to the seabed, including dynamically supported craft, submersibles, or any other floating craft.</p> <p>Convention: Article 2</p> <p>1. This Convention does not apply to:</p> <p>(a) a warship; or</p> <p>(b) a ship owned or operated by a State when being used as a naval auxiliary or for customs or police purposes; or</p> <p>(c) a ship which has been withdrawn from navigation or laid up.</p> <p>2. Nothing in this Convention affects the immunities of warships and other government ships operated for non-commercial purposes.</p> <p>Protocol: Article 1.3</p> <p>For the purposes of this Protocol, "fixed platform" means an artificial island, installation or structure permanently attached to the seabed for the purpose of exploration or exploitation of resources or for other economic purposes.</p>	<p>Articles 179 and 181</p> <p>Insertion of the term "boat" in the Articles 179 (Hijacking of a ship or an airplane) and 181 (Endangering the safety of the international air traffic and the international sea navigation) in order to encompass small watercraft.</p>

The Criminal Law is the main law (*lex generalis*) regulating the issues that SUA Convention deals with. This law uses the term ship, but it doesn't define it. The term ship has a legal meaning in Croatian legal system since it is defined in the Maritime Code:

"Ship, with the exception of warship is any waterborne craft intended for seagoing navigation, exceeding 12 meters in length and gross tonnage of 15 tons, or authorized to carry more than 12 passengers".⁴

It is also defined in the Law of Inland Waters (*lex specialis* in relation to the Maritime Code) in a similar way, except there is no criterion of seagoing navigation. Even the normal colloquial meaning of the term ship refers to a larger vessel, since the language differentiates between a ship and a boat. This, however, means that the term ship in Croatian law is narrower than the term ship in SUA Convention. The latter also encompasses what in Croatian law is considered a boat ("Boat is a waterborne craft intended for seaborne navigation that is not a ship."⁵), which in other words covers all the small seagoing craft. Therefore when the Criminal Law refers only to ship, it should be amended to cover any waterborne craft intended for seagoing navigation except a warship or a ship used in public services.

The Criminal Law, instead of "fixed platforms" uses the term "floating facility". The definition of this term according to the Maritime Code reads as follows: "*floating facility is a contrivance permanently moored or anchored, or fixed to the seabed and which is not capable of navigating (e.g. restaurants, landing stages, workshops, warehouses, pontoon bridges, pontoon marinas, offshore fixed platforms or drilling rigs, etc.)*;" Therefore, floating facility in Croatian law would encompass the term "fixed platforms" as used in the Protocol.

2. QUALIFICATION OF CRIMINAL OFFENCES

SUA Convention & Protocol	The Criminal Law	The Criminal Law (as amended)
<p>Convention: Article 3</p> <p>1. Any person commits an offence if that person unlawfully and intentionally:</p> <p>(a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; or</p> <p>(b) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; or</p>	<p>Article 179 <i>Hijacking of a ship or an airplane</i></p> <p>1. A person who takes control over an airplane during flight, a ship or a floating facility, by force or a serious threat thereof shall be punished by minimum one year imprisonment.</p> <p>2. If by committing a criminal offence from paragraph 1. of this article, the offender kills one or more persons, the offender shall be punished by</p>	<p>Article 179 (as amended): <i>Hijacking of a ship or an airplane</i></p> <p>1. A person who <i>seizes or exercises control</i> over an airplane during flight, or over a ship, <i>boat</i> or a floating facility, by force or a serious threat thereof <i>or any other form of intimidation</i> shall be punished by minimum one year imprisonment.</p> <p>2. If by committing a criminal offence from paragraph 1. of this article, the offender kills</p>

⁴ Maritime Code of the republic of Croatia, 1994, Art.5.2.

⁵ *ibid.* Art. 5.9.

<p>(c) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; or</p> <p>(d) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; or</p> <p>(e) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship; or</p> <p>(f) communicates information which he knows to be false, thereby endangering the safe navigation of a ship; or</p> <p>(g) injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f).</p> <p>2. Any person also commits an offence if that person:</p> <p>(a) attempts to commit any of the offences set forth in paragraph 1; or</p> <p>(b) abets the commission of any of the offences set forth in paragraph 1 perpetrated by</p>	<p>minimum 10 years or by long term imprisonment.⁶</p> <p>3. If a criminal offence from paragraph 1. of this article caused death of one or more persons or destruction of the airplane, ship, or the floating facility, or other large material damage the offender shall be punished by minimum 5 years imprisonment.</p> <p style="text-align: center;">Article 181 <i>Endangering the safety of the international air traffic and the international sea navigation</i></p> <p>1. (IRRELEVANT)</p> <p>2. (IRRELEVANT)</p> <p>3. A person who without the intention of hijacking a ship or a floating facility (art. 179) or committing a criminal offence of piracy (art. 180)⁷ puts in danger the safe navigation of the ship or the safety of the floating facility by destroying or damaging the navigational facilities or otherwise damaging the ship or the floating facility, placing or bringing on board the ship or the floating facility explosive or other device or substances which are likely to destroy or</p>	<p>one or more persons, the offender shall be punished by minimum 10 years or by long term imprisonment.</p> <p>3. If a criminal offence from paragraph 1. of this article caused death of one or more persons or destruction of the airplane, ship, <i>boat</i> or the floating facility, or other large material damage the offender shall be punished by minimum 5 years imprisonment.</p> <p><i>4. An attempt to commit any of the acts from this article shall be punished.</i></p> <p style="text-align: center;">Article 181 (as amended) <i>Endangering the safety of the international air traffic and the international sea navigation</i></p> <p>1. (IRRELEVANT)</p> <p>2. (IRRELEVANT)</p> <p>3. A person who without the intention of hijacking a ship <i>or boat</i> or a floating facility (art. 179) or committing a criminal offence of piracy (art. 180) puts in danger <i>or is likely to endanger</i> the safe navigation of the ship, <i>or boat</i> or the safety of the floating facility</p> <p>a. by destroying or <i>seriously</i> damaging the navigational facilities <i>or by interfering with their operation</i>, or otherwise <i>causing damage</i> to the ship <i>or its cargo or to the boat</i> or the</p>
--	---	--

⁶ Punishment by imprisonment in the Croatian Criminal Law cannot be shorter than 30 days or longer than 15 years. However, for very grave criminal offences a long-term imprisonment can be prescribed. Long-term imprisonment is 20-40 years in prison.

⁷ Art. 180. of the Criminal Law qualifies the crime of piracy as it is defined in the Law of the Sea Convention 1982, therefore *piracy jure gentium*.

<p>any person or is otherwise an accomplice of a person who commits such an offence; or</p> <p>(c) threatens, with or without a condition, as is provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraph 1, subparagraphs (b), (c) and (e), if that threat is likely to endanger the safe navigation of the ship in question.</p> <p>Protocol: Article 2</p> <p>1. Any person commits an offence if that person unlawfully and intentionally:</p> <p>(a) seizes or exercises control over a fixed platform by force or threat thereof or any other form of intimidation; or</p> <p>(b) performs an act of violence against a person on board a fixed platform if that act is likely to endanger its safety; or</p> <p>(c) destroys a fixed platform or causes damage to it which is likely to endanger its safety; or</p> <p>(d) places or causes to be placed on a fixed platform, by any means whatsoever, a device or substance which is likely to destroy that fixed platform or likely to endanger its safety; or</p> <p>(e) injures or kills any person in connection with the commission or the attempted commission of any of the</p>	<p>damage the ship or the floating facility, by giving out false information in connection with the navigation of the ship or the condition of the floating facility, by violent acts against the crew members of the ship or the floating facility or by other violent acts shall be punished by imprisonment from paragraph 1. of this article.⁸</p> <p>4. If a criminal offence from paragraph 1., 2. or 3. of this article caused death of one or more persons or destruction of the airplane, ship or the floating facility or serious damage to them or other large material damage, the offender shall be punished by minimum 3 years imprisonment.</p>	<p>floating facility,</p> <p>b. by placing, <i>causing to be placed</i> or bringing on board the ship, <i>boat</i> or the floating facility, <i>by any means whatsoever</i>, explosive or other device or substances which are likely to destroy or damage the ship <i>or its cargo, the boat</i> or the floating facility,</p> <p>c. by <i>knowingly</i> giving out the false information in connection with the navigation of the ship <i>or boat</i> or the condition of the floating facility,</p> <p>d. <i>by performing an act of violence against a crew member or other persons on board the ship, boat or floating facility or other violent acts,</i></p> <p>e. <i>or by a threat to commit any of the acts from subparagraphs a. and d. of this paragraph</i></p> <p>shall be punished by imprisonment from paragraph 1. of this article.</p> <p>4. If a criminal offence from paragraph 1., 2. or 3. of this article caused death of one or more persons or destruction of the airplane, ship, <i>boat</i> or the floating facility or serious damage to them or other large material damage,</p> <p>the offender shall be punished by minimum 3 years imprisonment.</p>
--	---	--

⁸ Paragraph 1. defines the offence of endangering the safety of the international air traffic. The punishment prescribed for that offence is 1-10 years of imprisonment.

<p>offences set forth in subparagraphs (a) to (d).</p> <p>2. Any person also commits an offence if that person:</p> <p>(a) attempts to commit any of the offences set forth in paragraph 1; or</p> <p>(b) abets the commission of any such offences perpetrated by any person or is otherwise an accomplice of a person who commits such an offence; or</p> <p>(c) threatens, with or without a condition, as is provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraph 1, subparagraphs (b) and (c), if that threat is likely to endanger the safety of the fixed platform.</p>	<p><i>5. If by committing a criminal offence from paragraph 1, 2. or 3. of this article, the offender kills one or more persons,</i></p> <p><i>the offender shall be punished by minimum 10 years or a long term imprisonment.</i></p> <p><i>6. An attempt to commit any of the acts from this article shall be punished.</i></p>
---	---

The offences of this nature are defined as criminal offences in the Criminal Law. The articles of the Criminal Law, however, should be amended to better implement the provisions of the SUA convention. The respective articles are inspired by the *International Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Montreal 1971*, and the *International Convention for the Suppression of Unlawful seizure of Aircraft, The Hague 1970*, to both of which Croatia is a party since 1993. The Criminal Law implements these conventions, but the drafters had also taken into account the SUA convention and its Protocol even though Croatia has not ratified them. In addition, SUA was actually patterned on the above mentioned 1971 Montreal Convention and the 1970 Hague Convention. For the economical purposes, the Croatian Criminal Law deals with the offences against security of air traffic and sea navigation together. The respective articles are placed in the Part XIII of the Criminal Law headed "Criminal Acts against the Values protected by the International Law". Their scope of application, however, sometimes extends also to the situations of internal nature, without the international element (e.g. the rules on hijacking of a ship extend to the domestic navigation, including the inland navigation).

ANALYSIS:

Art. 3. 1. of SUA Convention starts with saying "Any person commits an offence if that person *unlawfully and intentionally*...". This means that in order for an act

to be considered an offence there must be a legal basis (the offence must be defined as such in a law) and the intention of the perpetrator. Croatian criminal law also requires the existence of this objective (legality) and subjective (guilt) element for the existence of a crime. A person is guilty of a crime if there is an intention (direct or indirect)⁹ or recklessness on his or her part. A general rule is that a person is always criminally liable for the intention, while in order to be criminally liable for recklessness it must be expressly included in the legal definition of the crime. When defining the respective crimes against the safety of maritime navigation the Croatian Criminal Law requires intention of the offender, just like SUA.

Art. 3. 1. a) of SUA Convention provides that an offence is to seize or exercise control over a ship by force or threat thereof or any other form of intimidation. This would correspond to article 179 of the Croatian Criminal Law that defines crime of hijacking. This article should be amended as follows:

"(1) A person who *seizes or exercises control* over an airplane during flight, or over a ship, boat¹⁰ or a floating facility, by force or a serious threat thereof *or any other form of intimidation*..."

Art. 3. 1. b) of SUA Convention provides that an offence is to perform an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship. This provision corresponds with article 181 paragraph 3. of the Criminal Law: "A person who... endangers the safe navigation of the ship or the safety of the floating facility... by violent acts against the crew members of the ship or the floating facility or by other violent acts..." The proposed amendment is:

"A person who... puts in danger *or is likely to endanger*¹¹ the safe navigation of a ship or a boat or the safety of a floating facility... *by performing an act of violence against a crew member or other person on board the ship, boat or floating facility or other violent acts...*"

Art. 3. 1. c) of SUA Convention provides that an offence is to destroy a ship or cause damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship. The corresponding rule can be found in article 181 par. 3. of the Criminal Law: "A person who... puts in danger the safe navigation of a ship or the safety of the floating facility by... damaging the ship or the floating facility..." and in par. 4. of the same article: "If a criminal offence from paragraph 1., 2., or 3. of this article caused... destruction of the airplane, ship or the floating facility or serious damage to them or

⁹ *Dolus directus* exists when the offender was aware of his act and wanted its commission. *Dolus eventualis* exists when the offender was aware that he might commit a crime by his conduct (that because of his conduct a prohibited consequence might occur) and he accepts it.

¹⁰ It is proposed to add the term boat because the term ship used in SUA is wider than the term ship in Croatian law and it encompasses what in Croatian maritime law is considered a boat, too.

¹¹ To put in danger by committing certain acts, as the wording of the domestic legislation states might not be interpreted and understood to include both the actual endangering of the safety, and the likeliness of endangering it. It seems that the legislator's position is that there is a presumption that the respective acts will always lead to endangering the safety, but to avoid any doubt, there is a proposal to insert the phrase "likely to endanger".

other large material damage..." However, the domestic rules as they are, among other inconsistencies with the text of SUA, do not include the damage to cargo as an offence against safety of navigation. The proposed amendments are:

"181. 3. A person who... puts in danger *or is likely to endanger* the safe navigation of the ship *or boat* or the safety of the floating facility by... *causing damage* to the ship *or its cargo or to the boat* or the floating facility..."

"181. 4. If a criminal offence from paragraph 1., 2. or 3. of this article caused... destruction of the airplane, ship, *boat* or the floating facility or serious damage to them or other large material damage..."

According to Art. 3. 1. d) in SUA Convention an offence is to place or cause to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship. The Criminal Law also provides for a similar situation in Art. 181 par. 3. "A person who... puts in danger the safe navigation of the ship or the safety of the floating facility by... placing or bringing on board the ship or the floating facility explosive or other device or substances which are likely to destroy or damage the ship or the floating facility..." This must be read in conjunction with the previously described par. 4. of the same article. The proposed amendment to the respective part of par. 3. is as follows:

"A person who... puts in danger *or is likely to endanger* the safe navigation of the ship *or boat* or the safety of the floating facility by... *placing, causing to be placed* or bringing on board the ship, *boat* or the floating facility, *by any means whatsoever*, an explosive or other device or substances which are likely to destroy or damage the ship *or its cargo, the boat* or the floating facility..."

Art. 3. 1. e) of SUA Convention provides that an offence is to destroy or seriously damage maritime navigational facilities or seriously interfere with their operation, if any such act is likely to endanger the safe navigation of a ship. The Criminal Law contains the rule in article 181 par. 3: "A person who... puts in danger the safe navigation of the ship or the safety of the floating facility by destroying or damaging the navigational facilities..." which should be amended as follows:

"A person who... puts in danger *or is likely to endanger* the safe navigation of the ship *or boat* or the safety of the floating facility by destroying or *seriously* damaging the navigational facilities *or by interfering with their operation*..."

Art. 3. 1. f) of SUA Convention provides that an offence is to communicate information knowing to be false and thereby endangering the safe navigation of a ship. The Criminal Law similarly provides in Art. 181 par. 3: "A person who... puts in danger the safe navigation of the ship or the safety of the floating facility... by giving out false information in connection with the navigation of the ship or the condition of the floating facility...". The proposed amendment in this respect is:

“A person who... puts in danger or is likely to endanger the safe navigation of the ship or boat or the safety of the floating facility... by knowingly giving out false information in connection with the navigation of the ship or boat or the condition of the floating facility...”

Finally, Art. 3. 1. g) provides that an offence is to injure or kill any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs a. to f.. The Criminal Law contains similar rules in article 179 paragraphs 2. and 3. which need not be amended, except to include the term boat. It also provides in article 181 par. 4: *“If a criminal offence from paragraph 1., 2. or 3. of this article caused death of one or more persons...”* However, this provision does not particularly qualify a situation where there is actual killing of persons as opposed to the accidental death in connection with the previously considered offences. Therefore an insertion of a new paragraph 5. is proposed, which would be modeled on Art. 179 par. 2. of the Criminal Law:

“Art. 181 par. 5. If by committing a criminal offence from paragraph 1., 2. or 3. of this article, the offender kills one or more persons,

the offender shall be punished by minimum 10 years or a long term imprisonment.”

In Art. 3. 2. a) SUA Convention provides that an attempt of any of the offences qualified in paragraph 1. of the same article will also constitute an offence. Likewise, abetting the commission of the respective offences or being an accomplice of a person committing it constitutes an offence, too (Art. 3. 2. b). Finally, threatening to commit an offence of violence against the persons on board (Art. 3. 1. b), of destruction or damage to the ship or cargo (Art. 3. 1. c) or of damage or interference with the navigational facilities (Art. 3. 1. e) if that threat is likely to endanger the safe navigation of the ship in question (Art. 3. 2. c).

As regards the **attempt** of an offence, in the Croatian Criminal Law there is a general rule that a person who intentionally begins carrying out of a criminal act, but does not accomplish it, shall be punished for an attempt of a criminal act if according to the Criminal Law for the respective criminal offence there is a prescribed punishment of minimum 5 years imprisonment or if the Law itself expressly prescribes a punishment for the attempt of the respective criminal act. There are some qualifications as for the voluntary surrender, or use of inadequate means for accomplishing the act, but in general a person who attempted a criminal offence is to be punished *as if he or she had accomplished the offence*, but the punishment can also be milder (then it is up to the court's discretion).¹² Therefore, it would be necessary to insert express provisions in the relevant articles of the Criminal Law to make the attempt of all the respective offences punishable (Art. 179 par. 4. and 181 par. 6. in the amended Criminal Law).

¹² Art. 33., The Criminal Law of the Republic of Croatia, 1997

As for the **abettors and accomplices**, the Criminal Law provides for the adequate rules of general nature that apply to all the criminal offences including those relevant for the implementation of SUA. These rules about criminal responsibility of the abettors, accessories, accomplices, etc. need not be amended.¹³

Regarding the **threat** to commit any of the respective offences, the Criminal Law treats a threat as a separate criminal offence¹⁴. However, that does not correspond with the threat as described in SUA. Therefore, an amendment in Art. 181 of the Criminal Law is proposed to include threat as an offence in certain circumstances (Art. 181 par. 3. e).

Finally, as regards the Protocol, as it is shown, the articles of the Criminal Law include the protection of the safety of floating facilities against the respective offences qualified.

3. ESTABLISHMENT OF JURISDICTION

SUA Convention & Protocol	The Criminal Law (as amended)
<p>Convention: Article 6</p> <p>1. Each State Party shall <i>take such measures as may be necessary to establish its jurisdiction</i> over the offences set forth in article 3 when the offence is committed:</p> <p>(a) against or on board a <i>ship flying the flag</i> of the State at the time the offence is committed; or</p> <p>(b) <i>in the territory</i> of that State, including its territorial sea; or</p> <p>(c) <i>by a national</i> of that State.</p> <p>2. A State Party <i>may</i> also establish its jurisdiction over any such offence when:</p> <p>(a) it is committed by a <i>stateless person whose habitual residence</i> is in that State; or</p>	<p>Article 13 (as amended)</p> <p><i>Application of Criminal Laws to the criminal offences committed on the territory of the Republic of Croatia, its ship or aircraft</i></p> <p>1. Criminal laws of the Republic of Croatia apply to any person who commits a criminal offence on its territory <i>as well as on any person committing a criminal offence on board or against a floating facility while it is located on the Continental Shelf of the Republic of Croatia.</i></p> <p>2. Criminal laws of the Republic of Croatia apply also to any person who commits a criminal offence <i>against or</i> on board of a Croatian ship, regardless of where the ship is at the time of the commission of the criminal offence.</p> <p>3. (IRRELEVANT)</p> <p>Article 14 (as amended)</p> <p><i>Application of Criminal Laws to the criminal offences committed outside the territory of the Republic of Croatia</i></p> <p>1. Criminal laws of the Republic of Croatia apply to any person who outside its territory commits:</p>

¹³ Art. 36, 37, 38, *ibid.*

¹⁴ Art. 129, *ibid.*

<p>(b) during its commission a national of that State is seized, threatened, injured or killed; or</p> <p>(c) it is committed in an attempt to compel that State to do or abstain from doing any act.</p> <p>Protocol: Article 3</p> <p>1. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 when the offence is committed:</p> <p>(a) against or on board a fixed platform while it is located on the continental shelf of that State; or</p> <p>(b) by a national of that State.</p> <p>2. A State Party may also establish its jurisdiction over any such offence when:</p> <p>(a) it is committed by a stateless person whose habitual residence is in that State;</p> <p>(b) during its commission a national of that State is seized, threatened, injured or killed; or</p> <p>(c) it is committed in an attempt to compel that State to do or abstain from doing any act.</p>	<p>a) any criminal offence against the Republic of Croatia from the part XII of this Law;</p> <p>b) any criminal offence of forgery of money or bills of exchange of the Republic of Croatia;</p> <p>c) any criminal offence which the Republic of Croatia is obliged to punish under the rules of international law, particularly international agreements;</p> <p>2. Criminal laws of the Republic of Croatia apply to any Croatian national <i>or a stateless person who has a habitual residence in Croatia</i> who outside its territory commits a criminal offence other than those contained in the paragraph 1 of this article.</p> <p>3. Criminal Laws of the Republic of Croatia shall apply to a foreigner who outside the territory of the Republic of Croatia commits any criminal offence against the Republic of Croatia or its national that is not contained in the provision from paragraph 1. of this article.</p> <p>4. Criminal laws of the Republic of Croatia shall apply to a foreigner who outside the territory of the Republic of Croatia commits a criminal offence against a foreign state or its national if according to the law of that state the respective criminal offence is punishable by minimum 5 years imprisonment.</p> <p>5. In the cases from paragraphs 2. and 3. of this article, the criminal laws of the Republic of Croatia shall apply only if the offender is present in the territory or is extradited to the Republic of Croatia, while in the case from paragraph 4. of this article only if the offender is present in the territory of the Republic of Croatia and is not extradited to another state.</p>
--	---

ANALYSIS:

As for the Art. 6. 1. a) of SUA Convention, the corresponding provision in the Criminal Law is the following:

The Criminal Law: Art. 13

2. Criminal laws of the Republic of Croatia apply also to any person who commits a criminal offence on board of a Croatian ship, regardless of where the ship is at the time of the commission of the criminal offence.

The proposed amendment is to include the acts against a Croatian ship, and not only those on board:

2. Criminal laws of the Republic of Croatia apply also to any person who commits a criminal offence *against or* on board of a Croatian ship, regardless of where the ship is at the time of the commission of the criminal offence.

Provisions in Art. 6. 1. b) of SUA Convention and Art. 3. a) of Protocol are correspondent to the following:

The Criminal Law: Art. 13

(1) Criminal laws of the Republic of Croatia apply to any person who commits a criminal offence on its territory.

While the SUA provision is encompassed in this provision (territorial sea is a part of Croatian territory), the Protocol provision is not, therefore the proposed amendment is:

1. Criminal laws of the Republic of Croatia apply to any person who commits a criminal offence on its territory *as well as on any person committing a criminal offence on board or against a floating facility while it is located on the Continental Shelf of the Republic of Croatia.*

Regarding the jurisdiction over the Croatian nationals, the application of Criminal laws to them is established in Art. 14 paragraph 2. of the Criminal Law.

Finally, there is one provision that would encompass any criminal offence committed outside the territory of Croatia, if that would be mandatory under international law:

The Criminal Law: Art. 14

1. Criminal laws of the Republic of Croatia apply to any person who outside its territory commits:

c) a criminal offence which the Republic of Croatia is obliged to punish under the rules of international law, particularly international agreements.

So far, all the cases of obligatory jurisdiction according to SUA Convention and Protocol have been covered. However, the following provisions are proposed to be amended to provide for the application of Croatian Criminal laws in cases listed as facultative in SUA (Art. 6.2. of the Convention and Art. 3.2. of the Protocol):

The Criminal Law: Art. 14

2. Criminal laws of the Republic of Croatia apply to any Croatian national *or a stateless person who has a habitual residence in Croatia* who outside its territory commits a criminal offence other than those contained in the paragraph 1 of this article.¹⁵

(The proposed amendment is written in *bold italics*).

Finally, the provisions from Art. 6. 2. b) and c) of the Convention and Art 3. 2. b) and c) of the Protocol correspond to a provision in paragraph 3) of the Art. 14. of the Criminal Law which does not need an amendment. Maybe it should also be said that in paragraph 4) of article 14. the Criminal law provides for a possibility to establish jurisdiction over a foreign person who commits a crime that has no connection with Croatia whatsoever, but is punishable in a foreign state by a minimum 5 years imprisonment (universal jurisdiction principle). However, Croatia can establish its jurisdiction in those cases only if the offender is present in the territory and is not extradited to another state.

From the presented material it follows that on the basis of the domestic legislation the jurisdiction of Croatia over the offences qualified by SUA Convention and Protocol will be established in all cases where the alleged offender is present in the Croatian territory and is not extradited to any of the other States Parties to the Convention which are entitled to establish the jurisdiction (Art. 6.4. of the Convention, Art. 3.4. of the Protocol).

4. AUT DEDERE, AUT PUNIRE (EITHER EXTRADITE, OR PROSECUTE)

SUA Convention & Protocol	Constitution	The Criminal Law
Convention: Article 10 1. The State Party in the territory of which the offender or the alleged offender is found shall, in cases to which article 6 applies, if it does not extradite him, be obliged,	Article 9 1. (IRRELEVANT) 2. No Croatian Citizen shall be exiled from the Republic of Croatia or deprived from citizenship, nor extradited to	Article 15 <i>Special issues regarding the institution of criminal proceedings for crimes committed within the territory of the Republic of Croatia</i>

¹⁵ The last part of the provision refers to the following provision: "Criminal laws of the Republic of Croatia apply to any person who outside its territory commits: (a) any criminal offence against the Republic of Croatia from the part XII of this Law; (b) any criminal offence of forgery of money or bills of exchange of the Republic of Croatia c) any criminal offence which the Republic of Croatia is obliged to punish under the rules of international law, particularly international agreements." (Part XII deals with specific crimes against the Republic of Croatia such as treason, crimes against its sovereignty and independence, its highest officials, etc). Basically these three categories of acts are grouped together in a different paragraph because in those cases Croatia will always be entitled to establish its jurisdiction independently of whether the offender is available to its authorities or not, whereas in the case of the above discussed paragraph 2 of the same article, the establishment of jurisdiction is possible only if the offender is available to the authorities either because the person enters the Croatian territory or is extradited to Croatia.

<p>without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State.</p> <p>2. Any person regarding whom proceedings are being carried out in connection with any of the offences set forth in article 3 shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided for such proceedings by the law of the State in the territory of which he is present.</p>	<p>another state.</p> <p style="text-align: center;">Article 33</p> <p>Foreign citizens and stateless persons may obtain asylum in the Republic of Croatia, unless they are prosecuted for non-political crimes and activities contrary to the basic principles of international. No alien lawfully within the territory of the Republic of Croatia shall be expelled or extradited to another state, except in pursuance of a decision made in accordance with an international treaty and law.</p>	<p>1. (IRRELEVANT)</p> <p>2. Where in case of application of criminal laws of the Republic of Croatia in pursuance of the provisions contained in Article 13 of this law, the offender is a foreign citizen, the criminal proceedings can be handed over to a foreign state under the condition of reciprocity.</p> <p>3. The State Attorney of the Republic of Croatia decides on handing over of the criminal proceedings in the cases contained in paragraph 2. of this article.</p>
--	---	---

The provision contained in Article 10 of SUA Convention, which *mutatis mutandis* applies to the offences qualified in the Protocol, is probably one of the most important innovations. It imposes an obligation upon the States parties to the Convention to either prosecute the perpetrators of the offences qualified in the Convention that are available in its territory or to extradite them to another State party that has established its jurisdiction over that person in relation to the unlawful act committed. The idea is to create a network where the States co-operate in the suppression of unlawful acts against maritime security and to avoid the possibility of escaping responsibility because of a lack of established jurisdiction.

As is understood from the presented relevant articles of the Constitution and the Criminal Law, there is no problem in implementing the principle *aut dare, aut punire* when the offender is a foreign citizen. Article 33 of the Constitution allows extradition of foreign citizens when that is a decision made in accordance with an international treaty and with the law. SUA being an international treaty would give the basis for legality of such decision. There seems to be no impediment whatsoever for extradition of foreigners who committed a crime outside the territory of the Republic of Croatia (Article 14, the Criminal Law), whereas the foreigners who committed a crime within its territory, on its ship or aircraft, can be extradited to another state on the basis of reciprocity and following a decision of the State Attorney. SUA creates reciprocal

relationships in that sense among all the parties and would therefore satisfy the described requirement.

However, regarding the extradition of Croatian citizens to other states, it is strictly prohibited by the Constitution, and this provision is very unlikely to be ever changed. Therefore in the case of Croatian citizens who are perpetrators of unlawful acts qualified in SUA, and over whom the Croatian criminal jurisdiction is established by the force of law, there would be no possibility of extradition to another State party. Croatia would then be obliged to prosecute them and if not, that would be a breach of an international obligation. One may argue that Croatia is anyway extraditing its nationals to the International Criminal Tribunal for former Yugoslavia (ICTY) and that it is a signatory to the Rome Statute of the International Criminal Court (ICC) which also requires extradition of the State's nationals. However, the Constitution prohibits extradition to other states, whereas ICTY and ICC are international tribunals.

It is believed that the existing legal framework in this respect is a sufficient base for efficient implementation of SUA. Croatian criminal jurisdiction is established by virtue of law, and whenever there is jurisdiction, Croatian State Attorney is obliged by the Law to institute proceedings *ex officio*. All the offences qualified in SUA being recognised as criminal offences under Croatian Criminal law, become prosecutable *ex officio*. In addition, Croatia is a party to the International Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Montreal 1971, and the International Convention for the Suppression of Unlawful seizure of Aircraft, The Hague 1970 since 1993. Both of these Conventions have a similar provision containing *aut dare, aut punire* principle.

Finally, as regards purely procedural matters of extradition, in Croatia these are regulated by several international multilateral agreements. The most important among them is the European Convention on Extradition of December 1957 with its 2 additional protocols of 1976 and 1978. (published in the Official Gazette "Narodne Novine"-International Agreements No. 14/1994). The requirements for extradition have been specified in the Article 512 of the Criminal Procedure Act in compliance with Article 2 of the European Convention on Extradition¹⁶ which reads as follows:

ARTICLE 2

EXTRADITABLE OFFENCES

1. Extradition shall be granted in respect of offences punishable under the laws of the requesting Party and of the requested Party by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty. Where a conviction and prison sentence have occurred or a detention order has been made in the territory of the requesting Party, the punishment award must have been for a period of at least four months.

¹⁶ "The implications for Council of Europe member states of the ratification of the Rome Statute of the International Criminal Court – Progress report by Croatia", September 2001, Strasbourg, Council of Europe, Consult/(2001)33

2. If the request for extradition includes several separate offences each of which is punishable under the laws of the requesting Party and the requested Party by deprivation of liberty or under a detention order, but of which some do not fulfill the condition with regard to the amount of punishment which may be awarded, the requested Party shall also have the right to grant extradition for the latter offences.

3. Any Contracting Party whose law does not allow extradition form certain of the offences referred to in paragraph 1 of this Article may, in so far as it is concerned, exclude such offences from the application of this Convention.

4. Any Contracting Party which wishes to avail itself of the right provided for in paragraph 3 of this Article shall, at the time of the deposit of its instrument of ratification or accession, transmit to the Secretary General of the council of Europe either a list of the offences for which extradition is allowed or a list of those for which it is excluded and shall at the same time indicate the legal provisions which allow or exclude extradition. The Secretary-General of the Council shall forward these lists to the other signatories.

5. If extradition is subsequently excluded in respect of other offences by the law of a Contracting Party, that Party shall notify the Secretary-General. The Secretary-General shall inform the other signatories. Such notification shall not take effect until three months from the date of its receipt by the Secretary-General.

6. Any Party which avails itself of the right provided for in paragraphs 4 or 5 of this Article may at any time apply this Convention to offences which have been excluded from it. It shall inform the Secretary-General of the council of such changes, and the Secretary-General shall inform the other signatories.

7. Any Party may apply" reciprocity in respect of any offences excluded from the application of the Convention under this Article.

Croatia made an only reservation – not to extradite its own nationals.

5. MASTER'S AUTHORITY

SUA Convention	The Maritime Code	The Maritime Code (as amended)
<p>Convention: Article 8</p> <p>1. The master of a ship of a State Party (the "flag State") may deliver to the authorities of any other State Party (the "receiving State") any person who he has reasonable grounds to believe has committed one of the offences set forth in article 3.</p> <p>2. The flag State shall ensure that the master of its ship is obliged, whenever practicable, and if possible before entering the territorial sea of the</p>	<p>Article 177</p> <p>1. If in the course of the voyage a crew member, passenger or any person on board commits a criminal offence, the shipmaster shall, according to the circumstances, take measures necessary to prevent or mitigate the occurrence of harmful consequences of the offence and hold the perpetrator to account.</p> <p>2. If there is a risk of perpetrator's repeating the</p>	<p>Article 177 (as amended)</p> <p>1. If in the course of the voyage, <i>at anchor or under way</i>, a crew member, passenger or any <i>other</i> person commits a criminal offence <i>on board or against the ship</i>, the shipmaster shall, according to the circumstances, take measures necessary to prevent or mitigate the occurrence of harmful consequences of the offence and hold the perpetrator to account.</p> <p>2. If there is a risk of</p>

<p>receiving State carrying on board any person whom the master intends to deliver in accordance with paragraph 1, to give notification to the authorities of the receiving State of his intention to deliver such person and the reasons therefore.</p> <p>3. The receiving State shall accept the delivery, except where it has grounds to consider that the Convention is not applicable to the acts giving rise to the delivery, and shall proceed in accordance with the provisions of article 7. Any refusal to accept a delivery shall be accompanied by a statement of the reasons for refusal.</p> <p>4. The flag State shall ensure that the master of its ship is obliged to furnish the authorities of the receiving State with the evidence in the master's possession which pertains to the alleged offence.</p> <p>5. A receiving State which has accepted the delivery of a person in accordance with paragraph 3 may, in turn, request the flag State to accept delivery of that person. The flag State shall consider any such request, and if it accedes to the request it shall proceed in accordance with article 7. If the flag State declines a request, it shall furnish the receiving State with a statement of the reasons therefore.</p>	<p>offence or of his escaping, the shipmaster shall order: restriction of the perpetrator's freedom of movement on board, or his arrest; examination of the perpetrator, witnesses, eye-witnesses and injured parties in order to determine all the circumstances under which the offence has been committed and the resulting consequences; taking the record of all the hearings and examinations; taking into custody as material evidence all the objects on which or by which the offence has been committed, or on which the traces of the criminal offence are visible and taking other measures to determine the circumstances under which the criminal offence has been committed.</p> <p>3. If the ship is in a foreign country, the shipmaster shall submit a report on the criminal offence committed to the diplomatic or consular mission of the Republic of Croatia in the State into whose port the ship has first entered. The shipmaster shall deal with the perpetrator in compliance with the instructions received from the diplomatic or consular mission of the Republic of Croatia.</p> <p>4. After arrival at the first Croatian port of call, the shipmaster shall hand the perpetrator over to the body of internal affairs in that port with the written report on the criminal offence committed and the records and objects referred to in paragraph 2. of this article.</p>	<p>perpetrator's repeating the offence or of his escaping, the shipmaster shall order: restriction of the perpetrator's freedom of movement on board, or his arrest. <i>In any case the shipmaster shall order:</i> examination of the perpetrator, witnesses, eye-witnesses and injured parties in order to determine all the circumstances under which the offence has been committed and the resulting consequences; taking the record of all the hearings and examinations; taking into custody as material evidence all the objects on which or by which the offence has been committed, or on which the traces of the criminal offence are visible and taking other measures to determine the circumstances under which the criminal offence has been committed.</p> <p>3. <i>If the next port of call</i> is in a foreign country, the shipmaster shall submit a report on the criminal offence committed to the diplomatic or consular mission of the Republic of Croatia <i>to the State into whose port the ship is to enter. Whenever practicable, the shipmaster shall submit the report before entering the territorial sea of the State in question.</i> The shipmaster shall deal with the perpetrator, <i>written reports, records and objects referred to in paragraph 2 of this article</i> in compliance with the instructions of the diplomatic or consular mission of the Republic of Croatia.</p> <p>4. <i>If the next port of call is a Croatian port,</i> the shipmaster</p>
---	--	---

	5. The measures referred to in paragraphs 2. and 4. of this article shall be recorded with comments in the ship's logbook.	shall hand the perpetrator over to the <i>competent</i> body of internal affairs in that port with the written report on the criminal offence committed and the records and objects referred to in paragraph 2. of this article. <i>5. All the measures ordered or taken by the shipmaster in connection to the criminal offence</i> shall be recorded with comments in the ship's logbook.
--	--	--

There are few proposals for amendments to the Article 177 of the Maritime Code in order to harmonize it with the article 8 of SUA Convention providing for a procedure that the shipmaster is entitled to undertake if an offence as qualified in the article 3 has been committed. The Article 177 of the Maritime Code deals with situations where any criminal offence under the Croatian Criminal Law has taken place on board, including those offences qualified in the afore analysed articles 179 and 181 that implement article 3 of SUA Convention and Article 2 of SUA Protocol.

ANALYSIS:

In paragraph 1. the amendments purport to clarify that the master's authorities shall arise in any case of criminal offence on board or against the ship, whether while the ship is under way or it is anchored, all in compliance with the provisions of SUA.

An amendment is proposed in paragraph 2. of Article 177 of the Maritime Code, so to ensure that the shipmaster orders examination of the perpetrator, witnesses and all the other necessary measures to determine all the circumstances under which the offence has been committed and the resulting consequences and to make sure that all the material evidence has been taken into custody. The difference is that under the existing wording of the provision it could be interpreted that the master would undertake these measures only in the cases where the perpetrator is likely to escape or repeat the criminal offence. That interpretation is not satisfactory and therefore to avoid any confusion, the amendment is proposed to oblige the master to undertake the respective measures in all cases where there has been a criminal offence. This of course equally applies to the criminal offences from SUA.

Further amendments are proposed in paragraph 3. of the same article in Maritime Code: "177. 3. *If the next port of call* is in a foreign country, the shipmaster shall submit a report on the criminal offence committed to the diplomatic or consular mission of the Republic of Croatia *to* the State into whose port the ship *is to enter...*" is proposed instead of : "If the ship is in a foreign country, the shipmaster shall submit a report on the criminal offence committed to the diplomatic or consular mission of the

Republic of Croatia in the State into whose port the ship has first entered...". The reasons are following:

a. **"If the next port of call is in a foreign country..."**. The relevant fact is the next port of call, and not where the ship currently is. The ship may well be on the High Seas at the time of occurrence of the offence, but heading towards a foreign country. Furthermore this change is also relevant for the possibility of informing the respective mission about the offence before entering the territorial sea of the State in question, as it is required in the respective Art. 8 of SUA Convention.

b. **"submit a report on the criminal offence committed to the diplomatic or consular mission of the Republic of Croatia to the State into whose port the ship is to enter..."**. One amendment is to have a diplomatic or consular mission of the Republic of Croatia **to** instead of **in** the State in question. This is due to a hypothetical possibility of not having a diplomatic or consular mission physically in the respective State, but having a mission in another (e.g. neighbouring) State that is responsible for both States. The relevant fact there is that the mission is a mission **to** a particular State in question even though it might be physically based in another State. The second amendment in this part of provision is the "port the ship is to enter" instead of the "port the ship has first entered..." reason being basically the same as the one for the amendment justified under point a. above. It is important to have the report submitted before the ship has entered the port. The mission will then instruct the master how to proceed. In the cases where the offences qualified in SUA and in articles 179 and 181 of the Croatian Criminal Law respectively the mission will be obliged to take the steps in compliance with the provisions of SUA. It will instruct the master either to deliver the perpetrator to the competent authorities in the respective foreign port together with all the evidence furnished or to deliver the person to the competent Croatian authorities in the next Croatian port of call. In the first scenario the mission will also instruct the master to inform the competent foreign state's authorities about the intention to deliver the perpetrator. The further steps to be taken in relation to the foreign State will be in the hands of the mission.

c. **"Whenever practicable, the shipmaster shall submit the report before entering the territorial sea of the State in question."** This is an insertion that will allow the mission to react in time and take steps as described under the point b.

d. **"The shipmaster shall deal with the perpetrator, written reports, records and objects referred to in paragraph 2 of this article in compliance with the instructions of the diplomatic or consular mission of the Republic of Croatia."** The provision has been extended to include the reports, records and material evidence, because under the provisions of SUA, Croatia shall have obligations regarding this material. It will have to ensure a mechanism to make the material available to the States that might have a legal interest in it.

e. **"If the next port of call is a Croatian port"**. For this amendment the same reasoning is used as for the amendment under point a.

f. **“All the measures ordered or taken by the shipmaster in connection to the criminal offence shall be recorded”**. The reason for this amendment is quite clear. It is believed that it is important to have all the measures undertaken by the master or at his order recorded in the logbook and not only those contained in paragraphs 2. and 4. as it stands in the current wording.

C. Commentary for the Reader

This paragraph is intended for a reader who has no sufficient insight into the Croatian domestic law. Having in mind that footnotes cannot be included in the legislation instruments, unless they are a part of the original text of the international instruments being ratified and published therein, some relevant provisions to which there are references throughout this package, are set forth below:

The Constitution:

Article 89

1. Before coming into force, laws and other rules and regulations of governmental bodies shall be published in Narodne Novine, the Official Gazette of the Republic of Croatia.
2. the rules and regulations of bodies vested with public authority shall, before coming into force, be publicised in an accessible way, in accordance with the law.
3. A law shall come into force at the earliest on the eighth day after its publication, unless otherwise specified by law or exceptionally justified reasons.
4. Laws and other regulations of governmental bodies and bodies vested with public authority shall not have a retroactive effect.
5. Only individual provisions of a law may have a retroactive effect for exceptionally justified reasons.

Article 138

International agreements shall be concluded, in conformity with the Constitution, law and the rules of international law depending on the nature and contents of the international agreement, within the authority of the Croatian Parliament, the President of the Republic and the Government of the Republic of Croatia.

Article 139

1. International agreements which entail the passage or amendment of laws, international agreements of military and political nature, and international agreements which financially commit the Republic of Croatia shall be subject to ratification by the Croatian Parliament.
2. (IRRELEVANT)

3. The President of the Republic shall sign the documents on ratification, admittance, approval or acceptance of international agreements ratified by the Croatian Parliament in conformity with sections 1. and 2. of this Article.

4. International agreements which are not subject to ratification by the Croatian Parliament are concluded by the President of the Republic at the proposal of the Government, or by the Government of the Republic of Croatia.

Article 140

International agreements concluded and ratified in accordance with the Constitution and made public, and which are in force, shall be part of the internal legal order of the Republic of Croatia and shall be above law in terms of legal effects. Their provisions may be changed or repealed only under conditions and in the way specified in them or in accordance with the general rules of international law.

The Law on Conclusion and Execution of International Agreements:

Article 26

Exchange or deposit of instruments of ratification, acceptance, approval or accession and other acts in relation to entering into force of an international agreement for the Republic of Croatia is in the competence of the Ministry of Foreign Affairs.

Article 30

1. An act of approval of an international agreement with the text of that international agreement, as well as any other international agreement, shall be published without delay in Narodne Novine, the Official Gazette of the Republic of Croatia.

2. International agreements shall be published in Croatian language. If none of the authentic languages is Croatian, the international agreement shall be published in one of the authentic languages and in translation into Croatian language.

3. When publishing an international agreement, all the relevant information regarding entry into force of that agreement shall be included, and if at the time of the publication the international agreement is not in force, the information about its entry into force shall be published subsequently, after its entry into force.

THE HOUSE OF REPRESENTATIVES OF THE CROATIAN STATE PARLIAMENT

On the basis of Article 89 of the Constitution of the Republic of Croatia, I issue

DECISION

**TO PROMULGATE THE ACT OF RATIFICATION OF
THE CONVENTION FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST
THE SAFETY OF MARITIME NAVIGATION, 1988 AND
THE PROTOCOL FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE
SAFETY OF FIXED PLATFORMS LOCATED ON THE CONTINENTAL SHELF, 1988**

I promulgate the Act of Ratification of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf that was adopted by the House of Representatives of the Croatian State Parliament on its session held dd.mm.yyyy.

Number: XX-XXX-XX-XXXX/Y
Zagreb, dd.mm.yyyy.

The President of the Republic of Croatia

ACT

**OF RATIFICATION OF THE
CONVENTION FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE
SAFETY OF MARITIME NAVIGATION, 1988
AND THE
PROTOCOL FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE
SAFETY OF FIXED PLATFORMS LOCATED ON THE CONTINENTAL SHELF, 1988**

Article 1.

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf that were adopted at the Diplomatic Conference of the International Maritime Organisation in Rome on 10th March, 1988 and entered into force on 1st March, 1992 is hereby ratified.

The Convention and Protocol are established in a single copy in the Arabic, Chinese, English, French, Russian and Spanish languages, each text being equally authentic.

Article 2.

The Convention and Protocol in the original English language copy and the translation into Croatian language read as follows:

CONVENTION FOR SUPPRESSION OF UNLAWFUL ACTS AGAINST THE SAFETY OF MARITIME NAVIGATION

Done at Rome, 10th March 1988

THE STATES PARTIES TO THIS CONVENTION,

HAVING IN MIND the purposes and principles of the Charter of the United Nations concerning the maintenance of international peace and security and the promotion of friendly relations and co-operation among States,

RECOGNIZING in particular that everyone has the right to life, liberty and security of person, as set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights,

DEEPLY CONCERNED about the world-wide escalation of acts of terrorism in all its forms, which endanger or take innocent human lives, jeopardize fundamental freedoms and seriously impair the dignity of human beings,

CONSIDERING that unlawful acts against the safety of maritime navigation jeopardize the safety of persons and property, seriously affect the operation of maritime services, and undermine the confidence of the peoples of the world in the safety of maritime navigation,

CONSIDERING that the occurrence of such acts is a matter of grave concern to the international community as a whole,

BEING CONVINCED of the urgent need to develop international co-operation between States in devising and adopting effective and practical measures for the prevention of all unlawful acts against the safety of maritime navigation, and the prosecution and punishment of their perpetrators,

RECALLING resolution 40/61 of the General Assembly of the United Nations of 9 December 1985 which, inter alia, "urges all States unilaterally and in co-operation with other States, as well as relevant United Nations organs, to contribute to the progressive elimination of causes underlying international terrorism and to pay special attention to all situations, including colonialism, racism and situations involving mass and flagrant violations of human rights and fundamental freedoms and those involving alien occupation, that may give rise to international terrorism and may endanger international peace and security",

RECALLING FURTHER that resolution 40/61 "unequivocally condemns, as criminal, all acts, methods and practices of terrorism wherever and by whomever committed, including those which jeopardize friendly relations among States and their security",

RECALLING ALSO that by resolution 40/61, the International Maritime Organization was invited to "study the problem of terrorism aboard or against ships with a view to making recommendations on appropriate measures",

HAVING IN MIND resolution A.584(14) of 20 November 1985, of the Assembly of the International Maritime Organization, which called for development of measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews,

NOTING that acts of the crew which are subject to normal shipboard discipline are outside the purview of this Convention,

AFFIRMING the desirability of monitoring rules and standards relating to the prevention and control of unlawful acts against ships and persons on board ships, with a view to updating them as necessary, and, to this effect, taking note with satisfaction of the Measures to Prevent Unlawful Acts against Passengers and Crews on Board Ships, recommended by the Maritime Safety Committee of the International Maritime Organization,

AFFIRMING FURTHER that matters not regulated by this Convention continue to be governed by the rules and principles of general international law,

RECOGNIZING the need for all States, in combating unlawful acts against the safety of maritime navigation, strictly to comply with rules and principles of general international law,

HAVE AGREED as follows:

Article 1

For the purposes of this Convention, "ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft.

Article 2

1. This Convention does not apply to:

(a) a warship; or

(b) a ship owned or operated by a State when being used as a naval auxiliary or for customs or police purposes; or

(c) a ship which has been withdrawn from navigation or laid up.

2. Nothing in this Convention affects the immunities of warships and other government ships operated for non-commercial purposes.

Article 3

1. Any person commits an offence if that person *unlawfully and intentionally*:

(a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; or

(b) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; or

(c) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; or

(d) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; or

(e) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship; or

(f) communicates information which he knows to be false, thereby endangering the safe navigation of a ship; or

(g) injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f).

2. Any person also commits an offence if that person:

(a) attempts to commit any of the offences set forth in paragraph 1; or

(b) abets the commission of any of the offences set forth in paragraph 1 perpetrated by any person or is otherwise an accomplice of a person who commits such an offence; or

(c) threatens, with or without a condition, as is provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraph 1, subparagraphs (b), (c) and (e), if that threat is likely to endanger the safe navigation of the ship in question.

Article 4

1. This Convention applies if the ship is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single State, or the lateral limits of its territorial sea with adjacent States.

2. In cases where the Convention does not apply pursuant to paragraph 1, it nevertheless applies when the offender or the alleged offender is found in the territory of a State Party other than the State referred to in paragraph 1.

Article 5

Each State Party shall *make the offences* set forth in article 3 *punishable by appropriate penalties* which take into account the grave nature of those offences.

Article 6

1. Each State Party shall *take such measures* as may be *necessary to establish its jurisdiction* over the offences set forth in article 3 when the offence is committed:

(a) against or on board a *ship flying the flag* of the State at the time the offence is committed; or

(b) *in the territory* of that State, including its territorial sea; or

(c) *by a national* of that State.

2. A State Party *may* also establish its jurisdiction over any such offence when:

(a) it is committed by a *stateless person whose habitual residence* is in that State; or

(b) during its commission a *national of that State is seized, threatened, injured or killed*; or

(c) it is committed in an *attempt to compel that State* to do or abstain from doing any act.

3. Any State Party which has established jurisdiction mentioned in paragraph 2 shall *notify the Secretary-General of the International Maritime Organization* (hereinafter referred to as "the Secretary-General"). If such State Party subsequently *rescinds that jurisdiction*, it shall *notify* the Secretary-General.

4. Each State Party *shall take such measures* as may be *necessary to establish its jurisdiction* over the offences set forth in article 3 in cases where the alleged offender is *present in its territory and it does not extradite him to any of the States Parties* which have established their jurisdiction in accordance with paragraphs 1 and 2 of this article.

5. This Convention does not exclude any criminal jurisdiction exercised in accordance with national law.

Article 7

1. Upon being satisfied that the circumstances so warrant, any State Party in the territory of which the offender or the alleged offender is present shall, in accordance with its law, take him into custody or take other measures to ensure his presence for such time as is necessary to enable any criminal or extradition proceedings to be instituted.
2. Such State shall immediately make a preliminary inquiry into the facts, in accordance with its own legislation.
3. Any person regarding whom the measures referred to in paragraph 1 are being taken shall be entitled to:
 - (a) communicate without delay with the nearest appropriate representative of the State of which he is a national or which is otherwise entitled to establish such communication or, if he is a stateless person, the State in the territory of which he has his habitual residence;
 - (b) be visited by a representative of that State.
4. The rights referred to in paragraph 3 shall be exercised in conformity with the laws and regulations of the State in the territory of which the offender or the alleged offender is present, subject to the proviso that the said laws and regulations must enable full effect to be given to the purposes for which the rights accorded under paragraph 3 are intended.
5. When a State Party, pursuant to this article, has taken a person into custody, it shall immediately notify the States which have established jurisdiction in accordance with article 6, paragraph 1 and, if it considers it advisable, any other interested States, of the fact that such person is in custody and of the circumstances which warrant his detention. The State which makes the preliminary inquiry contemplated in paragraph 2 of this article shall promptly report its findings to the said States and shall indicate whether it intends to exercise jurisdiction.

Article 8

1. The master of a ship of a State Party (the "flag State") may deliver to the authorities of any other State Party (the "receiving State") any person who he has reasonable grounds to believe has committed one of the offences set forth in article 3.
2. The flag State shall ensure that the master of its ship is obliged, whenever practicable, and if possible before entering the territorial sea of the receiving State carrying on board any person whom the master intends to deliver in accordance with paragraph 1, to give notification to the authorities of the receiving State of his intention to deliver such person and the reasons therefore.

3. The receiving State shall accept the delivery, except where it has grounds to consider that the Convention is not applicable to the acts giving rise to the delivery, and shall proceed in accordance with the provisions of article 7. Any refusal to accept a delivery shall be accompanied by a statement of the reasons for refusal.

4. The flag State shall ensure that the master of its ship is obliged to furnish the authorities of the receiving State with the evidence in the master's possession which pertains to the alleged offence.

5. A receiving State which has accepted the delivery of a person in accordance with paragraph 3 may, in turn, request the flag State to accept delivery of that person. The flag State shall consider any such request, and if it accedes to the request it shall proceed in accordance with article 7. If the flag State declines a request, it shall furnish the receiving State with a statement of the reasons therefore.

Article 9

Nothing in this Convention shall affect in any way the rules of international law pertaining to the competence of States to exercise investigative or enforcement jurisdiction on board ships not flying their flag.

Article 10

1. The State Party in the territory of which the offender or the alleged offender is found shall, in cases to which article 6 applies, if it does not extradite him, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State.

2. Any person regarding whom proceedings are being carried out in connection with any of the offences set forth in article 3 shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided for such proceedings by the law of the State in the territory of which he is present.

Article 11

1. The offences set forth in article 3 shall be deemed to be included as extraditable offences in any extradition treaty existing between any of the States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.

2. If a State Party which makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, the requested State Party may, at its option, consider this

Convention as a legal basis for extradition in respect of the offences set forth in article 3. Extradition shall be subject to the other conditions provided by the law of the requested State Party.

3. States Parties which do not make extradition conditional on the existence of a treaty shall recognize the offences set forth in article 3 as extraditable offences between themselves, subject to the conditions provided by the law of the requested State.

4. If necessary, the offences set forth in article 3 shall be treated, for the purposes of extradition between States Parties, as if they had been committed not only in the place in which they occurred but also in a place within the jurisdiction of the State Party requesting extradition.

5. A State Party which receives more than one request for extradition from States which have established jurisdiction in accordance with article 6 and which decides not to prosecute shall, in selecting the State to which the offender or alleged offender is to be extradited, pay due regard to the interests and responsibilities of the State Party whose flag the ship was flying at the time of the commission of the offence.

6. In considering a request for the extradition of an alleged offender pursuant to this Convention, the requested State shall pay due regard to whether his rights as set forth in article 7, paragraph 3, can be effected in the requesting State.

7. With respect to the offences as defined in this Convention, the provisions of all extradition treaties and arrangements applicable between States Parties are modified as between States Parties to the extent that they are incompatible with this Convention.

Article 12

1. State Parties shall afford one another the greatest measure of assistance in connection with criminal proceedings brought in respect of the offences set forth in article 3, including assistance in obtaining evidence at their disposal necessary for the proceedings.

2. States Parties shall carry out their obligations under paragraph 1 in conformity with any treaties on mutual assistance that may exist between them. In the absence of such treaties, States Parties shall afford each other assistance in accordance with their national law.

Article 13

1. States Parties shall co-operate in the prevention of the offences set forth in article 3, particularly by:

(a) taking all practicable measures to prevent preparations in their respective territories for the commission of those offences within or outside their territories;

(b) exchanging information in accordance with their national law, and co-ordinating administrative and other measures taken as appropriate to prevent the commission of offences set forth in article 3.

2. When, due to the commission of an offence set forth in article 3, the passage of a ship has been delayed or interrupted, any State Party in whose territory the ship or passengers or crew are present shall be bound to exercise all possible efforts to avoid a ship, its passengers, crew or cargo being unduly detained or delayed.

Article 14

Any State Party having reason to believe that an offence set forth in article 3 will be committed shall, in accordance with its national law, furnish as promptly as possible any relevant information in its possession to those States which it believes would be the States having established jurisdiction in accordance with article 6.

Article 15

1. Each State Party shall, in accordance with its national law, provide to the Secretary-General, as promptly as possible, any relevant information in its possession concerning:

(a) the circumstances of the offence;

(b) the action taken pursuant to article 13, paragraph 2;

(c) the measures taken in relation to the offender or the alleged offender and, in particular, the results of any extradition proceedings or other legal proceedings.

2. The State Party where the alleged offender is prosecuted shall, in accordance with its national law, communicate the final outcome of the proceedings to the Secretary-General.

3. The information transmitted in accordance with paragraphs 1 and 2 shall be communicated by the Secretary-General to all States Parties, to Members of the International Maritime Organization (hereinafter referred to as "the Organization"), to the other States concerned, and to the appropriate international intergovernmental organizations.

Article 16

1. Any dispute between two or more States Parties concerning the interpretation or application of this Convention which cannot be settled through negotiation within a reasonable time shall, at the request of one of them, be submitted to arbitration. If, within six months from the date of the request for arbitration, the parties are unable to agree on the organization of the arbitration any one of those parties may refer the dispute to the International Court of Justice by request in conformity with the Statute of the Court.

2. Each State may at the time of signature or ratification, acceptance or approval of this Convention or accession thereto, declare that it does not consider itself bound by any or all of the provisions of paragraph 1. The other States Parties shall not be bound by those provisions with respect to any State Party which has made such a reservation.

3. Any State which has made a reservation in accordance with paragraph 2 may, at any time, withdraw that reservation by notification to the Secretary-General.

Article 17

1. This Convention shall be open for signature at Rome on 10 March 1988 by States participating in the International Conference on the Suppression of Unlawful Acts against the Safety of Maritime Navigation and at the Headquarters of the Organization by all States from 14 March 1988 to 9 March 1989. It shall thereafter remain open for accession.

2. States may express their consent to be bound by this Convention by:

(a) signature without reservation as to ratification, acceptance or approval; or

(b) signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval; or

(c) accession.

3. Ratification, acceptance, approval or accession shall be effected by the deposit of an instrument to that effect with the Secretary-General.

Article 18

1. This Convention shall enter into force ninety days following the date on which fifteen States have either signed it without reservation as to ratification, acceptance or approval, or have deposited an instrument of ratification, acceptance, approval or accession in respect thereof.

2. For a State which deposits an instrument of ratification, acceptance, approval or accession in respect of this Convention after the conditions for entry into force thereof have been met, the ratification, acceptance, approval or accession shall take effect ninety days after the date of such deposit.

Article 19

1. This Convention may be denounced by any State Party at any time after the expiry of one year from the date on which this Convention enters into force for that State.

2. Denunciation shall be effected by the deposit of an instrument of denunciation with the Secretary-General.

3. A denunciation shall take effect one year, or such longer period as may be specified in the instrument of denunciation, after the receipt of the instrument of denunciation by the Secretary-General.

Article 20

1. A conference for the purpose of revising or amending this Convention may be convened by the Organization.

2. The Secretary-General shall convene a conference of the States Parties to this Convention for revising or amending the Convention, at the request of one third of the States Parties, or ten States Parties, whichever is the higher figure.

3. Any instrument of ratification, acceptance, approval or accession deposited after the date of entry into force of an amendment to this Convention shall be deemed to apply to the Convention as amended.

Article 21

1. This Convention shall be deposited with the Secretary-General.

2. The Secretary-General shall:

(a) inform all States which have signed this Convention or acceded thereto, and all Members of the Organization, of:

(i) each new signature or deposit of an instrument of ratification, acceptance, approval or accession together with the date thereof;

(ii) the date of the entry into force of this Convention;

(iii) the deposit of any instrument of denunciation of this Convention together with the date on which it is received and the date on which the denunciation takes effect;

(iv) the receipt of any declaration or notification made under this Convention;

(b) transmit certified true copies of this Convention to all States which have signed this Convention or acceded thereto.

3. As soon as this Convention enters into force, a certified true copy thereof shall be transmitted by the Depositary to the Secretary-General of the United Nations for registration and publication in accordance with Article 102 of the Charter of the United Nations.

Article 22

This Convention is established in a single original in the Arabic, Chinese, English, French, Russian and Spanish languages, each text being equally authentic.

IN WITNESS WHEREOF the undersigned being duly authorized by their respective Governments for that purpose have signed this Convention.

DONE AT ROME this tenth day of March one thousand nine hundred and eighty-eight.

PROTOCOL FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE SAFETY OF FIXED PLATFORMS LOCATED ON THE CONTINENTAL SHELF

Done at Rome, 10 March 1988

THE STATES PARTIES TO THIS PROTOCOL,

BEING PARTIES to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,

RECOGNIZING that the reasons for which the Convention was elaborated also apply to fixed platforms located on the continental shelf,

TAKING ACCOUNT of the provisions of that Convention,

AFFIRMING that matters not regulated by this Protocol continue to be governed by the rules and principles of general international law,

HAVE AGREED as follows:

Article 1

1. The provisions of articles 5 and 7 and of articles 10 to 16 of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (hereinafter referred to as "the Convention") shall also apply mutatis mutandis to the offences set forth in article 2 of this Protocol where such offences are committed on board or against fixed platforms located on the continental shelf.

2. In cases where this Protocol does not apply pursuant to paragraph 1, it nevertheless applies when the offender or the alleged offender is found in the territory of a State Party other than the State in whose internal waters or territorial sea the fixed platform is located.

3. For the purposes of this Protocol, "fixed platform" means an artificial island, installation or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.

Article 2

1. Any person commits an offence if that person unlawfully and intentionally:

(a) seizes or exercises control over a fixed platform by force or threat thereof or any other form of intimidation; or

(b) performs an act of violence against a person on board a fixed platform if that act is likely to endanger its safety; or

(c) destroys a fixed platform or causes damage to it which is likely to endanger its safety; or

(d) places or causes to be placed on a fixed platform, by any means whatsoever, a device or substance which is likely to destroy that fixed platform or likely to endanger its safety; or

(e) injures or kills any person in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (d).

2. Any person also commits an offence if that person:

(a) attempts to commit any of the offences set forth in paragraph 1; or

(b) abets the commission of any such offences perpetrated by any person or is otherwise an accomplice of a person who commits such an offence; or

(c) threatens, with or without a condition, as is provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraph 1, subparagraphs (b) and (c), if that threat is likely to endanger the safety of the fixed platform.

Article 3

1. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 when the offence is committed:

(a) against or on board a fixed platform while it is located on the continental shelf of that State; or

(b) by a national of that State.

2. A State Party may also establish its jurisdiction over any such offence when:

- (a) it is committed by a stateless person whose habitual residence is in that State;
- (b) during its commission a national of that State is seized, threatened, injured or killed;
or
- (c) it is committed in an attempt to compel that State to do or abstain from doing any act.

3. Any State Party which has established jurisdiction mentioned in paragraph 2 shall notify the Secretary-General of the International Maritime Organization (hereinafter referred to as "the Secretary-General"). If such State Party subsequently rescinds that jurisdiction, it shall notify the Secretary-General.

4. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 in cases where the alleged offender is present in its territory and it does not extradite him to any of the States Parties which have established their jurisdiction in accordance with paragraphs 1 and 2 of this article.

5. This Protocol does not exclude any criminal jurisdiction exercised in accordance with national law.

Article 4

Nothing in this Protocol shall affect in any way the rules of international law pertaining to fixed platforms located on the continental shelf.

Article 5

1. This Protocol shall be open for signature at Rome on 10 March 1988 and at the Headquarters of the International Maritime Organization (hereinafter referred to as "the Organization") from 14 March 1988 to 9 March 1989 by any State which has signed the Convention. It shall thereafter remain open for accession.

2. States may express their consent to be bound by this Protocol by:

- (a) signature without reservation as to ratification, acceptance or approval; or
- (b) signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval; or
- (c) accession.

3. Ratification, acceptance, approval or accession shall be effected by the deposit of an instrument to that effect with the Secretary-General.

4. Only a State which has signed the Convention without reservation as to ratification, acceptance or approval, or has ratified, accepted, approved or acceded to the Convention may become a Party to this Protocol.

Article 6

1. This Protocol shall enter into force ninety days following the date on which three States have either signed it without reservation as to ratification, acceptance or approval, or have deposited an instrument of ratification, acceptance, approval or accession in respect thereof. However, this Protocol shall not enter into force before the Convention has entered into force.

2. For a State which deposits an instrument of ratification, acceptance, approval or accession in respect of this Protocol after the conditions for entry into force thereof have been met, the ratification, acceptance, approval or accession shall take effect ninety days after the date of such deposit.

Article 7

1. This Protocol may be denounced by any State Party at any time after the expiry of one year from the date on which this Protocol enters into force for that State.

2. Denunciation shall be effected by the deposit of an instrument of denunciation with the Secretary-General.

3. A denunciation shall take effect one year, or such longer period as may be specified in the instrument of denunciation, after the receipt of the instrument of denunciation by the Secretary-General.

4. A denunciation of the Convention by a State Party shall be deemed to be a denunciation of this Protocol by that Party.

Article 8

1. A conference for the purpose of revising or amending this Protocol may be convened by the Organization.

2. The Secretary-General shall convene a conference of the States Parties to this Protocol for revising or amending the Protocol, at the request of one third of the States Parties, or five States Parties, whichever is the higher figure.

3. Any instrument of ratification, acceptance, approval or accession deposited after the date of entry into force of an amendment to this Protocol shall be deemed to apply to the Protocol as amended.

Article 9

1. This Protocol shall be deposited with the Secretary-General.

2. The Secretary-General shall:

(a) inform all States which have signed this Protocol or acceded thereto, and all Members of the Organization, of:

(i) each new signature or deposit of an instrument of ratification, acceptance, approval or accession, together with the date thereof;

(ii) the date of entry into force of this Protocol;

(iii) the deposit of any instrument of denunciation of this Protocol together with the date on which it is received and the date on which the denunciation takes effect;

(iv) the receipt of any declaration or notification made under this Protocol or under the Convention, concerning this Protocol;

(b) transmit certified true copies of this Protocol to all States which have signed this Protocol or acceded thereto.

3. As soon as this Protocol enters into force, a certified true copy thereof shall be transmitted by the Depositary to the Secretary-General of the United Nations for registration and publication in accordance with Article 102 of the Charter of the United Nations.

Article 10

This Protocol is established in a single original in the Arabic, Chinese, English, French, Russian and Spanish languages, each text being equally authentic.

IN WITNESS WHEREOF the undersigned, being duly authorized by their respective Governments for that purpose, have signed this Protocol.

DONE AT ROME this tenth day of March one thousand nine hundred and eighty-eight.

Article 3.

The competent authorities for the execution of the Convention and Protocol set forth in Article 2. of this Act are the Ministry of Justice, Public Administration and Local Self-government of the Republic of Croatia, The Ministry of Internal Affairs of the Republic of Croatia, and the judicial bodies of the Republic of Croatia.

Article 4.

The Convention and Protocol set forth in Article 2. of this Act shall not be in force for the Republic of Croatia on the day of entry into force of this Act. The information about the entry into force of this Convention and Protocol shall be announced subsequently in accordance with Article 30. paragraph 3. of the Law on Conclusion and Execution of International Agreements ("Narodne Novine", No. 28/96) after their entry into force.

Article 5.

This Act shall enter into force on the 8th day from its publication in "Narodne Novine".

Class: XXX-XX/XX-XX/XX
Zagreb, dd.mm.yyyy.

HOUSE OF REPRESENTATIVES OF THE CROATIAN STATE PARLIAMENT

President

of the House of Representatives of the Croatian State Parliament

THE MINISTRY OF FOREIGN AFFAIRS

On the basis of Article 26. and Article 30. paragraph 3. of the Law on Conclusion and Execution of International Agreements ("Narodne novine", No. 28/96), the Ministry of Foreign Affairs of the Republic of Croatia

ANNOUNCES

That the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf that were adopted at the Diplomatic Conference of the International Maritime Organisation in Rome on 10th March, 1988 entered into force on 1st March, 1992 and published in "Narodne Novine – International Agreements" No. XX/YY, entered into force for the Republic of Croatia on the date of accession dd.mm.yyyy.

Class: XXX-XX/XX-XX/XX

Reg. Number: XXX-XX-XX-XX/XX-XX-XX

Zagreb, dd.mm.yyyy.

The Minister of Foreign Affairs

THE HOUSE OF REPRESENTATIVES OF THE CROATIAN STATE PARLIAMENT

On the basis of Article 89. of the Constitution of the Republic of Croatia, I issue

DECISION

TO PROMULGATE THE LAW ON THE AMENDMENTS TO THE CRIMINAL LAW

I promulgate the Law on the Amendments to the Criminal Law that was adopted by the House of Representatives of the Croatian State Parliament on its session of dd.mm.yyyy.

Number:
Zagreb,

President Of the Republic of Croatia

LAW

ON THE AMENDMENTS TO THE CRIMINAL LAW

Article 1.

Article 13. paragraphs 1. and 2. are amended and read:

(1) Criminal laws of the Republic of Croatia apply to any person who commits a criminal offence on its territory as well as on any person committing a criminal offence on board or against a floating facility while it is located on the Continental Shelf of the Republic of Croatia.

(2) Criminal laws of the Republic of Croatia apply also to any person who commits a criminal offence against or on board of a Croatian ship, regardless of where the ship is at the time of the commission of the criminal offence.

Article 2.

Article 14. paragraph 2. is amended and reads:

(2) Criminal laws of the Republic of Croatia apply to any Croatian national or a stateless person who has a habitual residence in Croatia who outside its territory commits a criminal offence other than those contained in the paragraph 1 of this article.

Article 3.

Article 179. paragraph 1. is amended and reads:

(1) A person who seizes or exercises control over an airplane during flight, or over a ship, boat or a floating facility, by force or a serious threat thereof or any other form of intimidation shall be punished by minimum one year imprisonment.

A new paragraph 4. is added:

(4) An attempt to commit any of the acts from this article shall be punished.

Article 4.

Article 181. paragraph 3. is amended and reads:

(3) A person who without the intention of hijacking a ship or boat or a floating facility (art. 179.) or committing the criminal offence of piracy (art. 180.) puts in danger or is likely to endanger the safe navigation of the ship or boat or the safety of the floating facility

a. by destroying or seriously damaging the navigational facilities or by interfering with their operation, or otherwise causing damage to the ship or its cargo or to the boat or the floating facility,

b. by placing, causing to be placed or bringing on board the ship, boat or the floating facility, by any means whatsoever, explosive or other device or substances which are likely to destroy or damage the ship or its cargo, the boat or the floating facility,

c. by knowingly giving out the false information in connection with the navigation of the ship or boat or the condition of the floating facility,

d. by performing an act of violence against a crew member or other persons on board the ship, boat or floating facility or other violent acts,

e. or by a threat to commit any of the acts from subparagraphs a. and d. of this paragraph

shall be punished by imprisonment from paragraph 1. of this article.

Paragraph 4. is amended and reads:

(4) If a criminal offence from paragraph 1. ,2. or 3. of this article caused death of one or more persons or destruction of the airplane, ship, boat or the floating facility or serious damage to them or other large material damage, the offender shall be punished by minimum 3 years imprisonment.

New paragraphs 5. and 6. are added:

(5) If by committing a criminal offence from paragraph 1., 2. or 3. of this article, the offender kills one or more persons, the offender shall be punished by minimum 10 years or a long term imprisonment.

(6) An attempt to commit any of the acts from this article shall be punished.

Article 5.

The Legislative Committee of the House of Representatives of the Croatian Parliament shall be competent for determining and issuing the full amended text of the Criminal Law.

Article 6.

This Law shall enter into force on the 8th day from its publication in "Narodne Novine".

Class:
Zagreb,

**THE HOUSE OF REPRESENTATIVES OF THE
CROATIAN STATE PARLIAMENT**

President
of the House of Representatives of the Croatian State Parliament

THE GOVERNMENT OF THE REPUBLIC OF CROATIA

On the basis of Article 30. paragraph 1. of the Law on Conclusion and Execution of International Agreements (»Narodne novine«, No. 28/96), the Government of the Republic of Croatia on its session held dd.mm.yyyy. issued

DECREE

TO PUBLISH THE AMENDMENTS TO THE ANNEX TO THE 1974 CONVENTION FOR THE SAFETY OF LIFE AT SEA

Article 1.

The Amendments to the Annex to the 1974 Convention for the Safety of Life at Sea that were adopted at the Diplomatic Conference on Maritime Security held in London from 9th to 13th December 2002 and established in a single copy in the Chinese, English, French, Russian and Spanish languages, each text being equally authentic, are hereby published.

Article 2.

The text of the Amendments mentioned in Article 1. of this Decree in the original English language copy and the translation into Croatian language reads as follows:

AMENDMENTS TO THE ANNEX TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 AS AMENDED

CHAPTER V SAFETY OF NAVIGATION

Regulation 19

Carriage requirements for shipborne navigational systems and equipment

1. The existing subparagraphs .4, .5 and .6 of paragraph 2.4.2 are replaced by the following:

“.4 in the case of ships, other than passenger ships and tankers, of 300 gross tonnage and upwards but less than 50,000 gross tonnage, not later than the first

safety equipment survey¹⁷ after 1 July 2004 or by 31 December 2004, whichever occurs earlier; and"

2. The following new sentence is added at the end of the existing subparagraph 7. of paragraph 2.4:

"Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information."

CHAPTER XI

SPECIAL MEASURES TO ENHANCE MARITIME SAFETY

3. The existing chapter XI is renumbered as chapter XI-1.

Regulation 3

Ship identification number

4. The following text is inserted after the title of the regulation:

"(Paragraphs 4 and 5 apply to all ships to which this regulation applies. For ships constructed before [1 July 2004], the requirements of paragraphs 4 and 5 shall be complied with not later than the first scheduled dry-docking of the ship after [1 July 2004])"

5. The existing paragraph 4 is deleted and the following new text is inserted:

"4. The ship's identification number shall be permanently marked:

.1 in a visible place either on the stern of the ship or on either side of the hull, amidships port and starboard, above the deepest assigned load line or either side of the superstructure, port and starboard or on the front of the superstructure or, in the case of passenger ships, on a horizontal surface visible from the air; and

.2 in an easily accessible place either on one of the end transverse bulkheads of the machinery spaces, as defined in regulation II-2/3.30, or on one of the hatchways or, in the case of tankers, in the pump-room or, in the case of ships with ro-ro spaces, as defined in regulation II-2/3.41, on one of the end transverse bulkheads of the ro-ro spaces.

- 5.1 The permanent marking shall be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting colour.

¹⁷ The first safety equipment survey means the first annual survey the first periodical survey or the first renewal survey for safety equipment, whichever is due first after 1 July 2004 and, in addition, in the case of ships under construction, the initial survey.

5.2 The permanent marking referred to in paragraph 4.1 shall be not less than 200 mm in height. The permanent marking referred to in paragraph 4.2 shall not be less than 100 mm in height. The width of the marks shall be proportionate to the height.

5.3 The permanent marking may be made by raised lettering or by cutting it in or by centre punching it or by any other equivalent method of marking the ship identification number which ensures that the marking is not easily expunged.

5.4 On ships constructed of material other than steel or metal, the Administration shall approve the method of marking the ship identification number.”

6. The following new regulation 5 is added after the existing regulation 4:

**“Regulation 5
Continuous Synopsis Record**

1 Every ship to which chapter I applies shall be issued with a Continuous Synopsis Record.

2.1 The Continuous Synopsis Record is intended to provide an on-board record of the history of the ship with respect to the information recorded therein.

2.2 For ships constructed before 1 July 2004, the Continuous Synopsis Record shall, at least, provide the history of the ship as from 1 July 2004.

3 The Continuous Synopsis Record shall be issued by the Administration to each ship that is entitled to fly its flag and it shall contain at least, the following information:

- .1 the name of the State whose flag the ship is entitled to fly;
- .2 the date on which the ship was registered with that State;
- .3 the ship’s identification number in accordance with regulation 3;
- .4 the name of the ship;
- .5 the port at which the ship is registered;
- .6 the name of the registered owner(s) and their registered address(es);
- .7 the name of the registered bareboat charterer(s) and their registered address(es), if applicable;

.8 the name of the Company, as defined in regulation IX/1, its registered address and the address(es) from where it carries out the safety management activities;

.9 the name of all classification society(ies) with which the ship is classed;

.10 the name of the Administration or of the Contracting Government or of the recognized organization which has issued the Document of Compliance (or the Interim Document of Compliance), specified in the ISM Code as defined in regulation IX/1, to the Company operating the ship and the name of the body which has carried out the audit on the basis of which the document was issued, if other than that issuing the document;

.11 the name of the Administration or of the Contracting Government or of the recognized organization that has issued the Safety Management Certificate (or the Interim Safety Management Certificate), specified in the ISM Code as defined in regulation IX/1, to the ship and the name of the body which has carried out the audit on the basis of which the certificate was issued, if other than that issuing the certificate;

.12 the name of the Administration or of the Contracting Government or of the recognized security organization that has issued the International Ship Security Certificate (or an Interim International Ship Security Certificate), specified in part A of the ISPS Code as defined in regulation XI-2/1, to the ship and the name of the body which has carried out the verification on the basis of which the certificate was issued, if other than that issuing the certificate; and

.13 the date on which the ship ceased to be registered with that State.

4.1 Any changes relating to the entries referred to in paragraphs 3.4 to 3.12 shall be recorded in the Continuous Synopsis Record so as to provide updated and current information together with the history of the changes.

4.2 In case of any changes relating to the entries referred to in paragraph 4.1, the Administration shall issue, as soon as is practically possible but not later than three months from the date of the change, to the ships entitled to fly its flag either a revised and updated version of the Continuous Synopsis Record or appropriate amendments thereto.

4.3 In case of any changes relating to the entries referred to in paragraph 4.1, the Administration, pending the issue of a revised and updated version of the Continuous Synopsis Record, shall authorise and require either the Company as defined in regulation IX/1 or the master of the ship to amend the Continuous Synopsis Record to reflect the changes. In such cases, after the Continuous

Synopsis Record has been amended the Company shall, without delay, inform the Administration accordingly.

5.1 The Continuous Synopsis Record shall be in English, French or Spanish language. Additionally, a translation of the Continuous Synopsis Record into the official language or languages of the Administration may be provided.

5.2 The Continuous Synopsis Record shall be in the format developed by the Organization and shall be maintained in accordance with guidelines developed by the Organization. Any previous entries in the Continuous Synopsis Record shall not be modified, deleted or, in any way, erased or defaced.

6 Whenever a ship is transferred to the flag of another State or the ship is sold to another owner (or is taken over by another bareboat charterer) or another Company assumes the responsibility for the operation of the ship, the Continuous Synopsis Record shall be left on board.

7 When a ship is to be transferred to the flag of another State, the Company shall notify the Administration of the name of the State under whose flag the ship is to be transferred so as to enable the Administration to forward to that State a copy of the Continuous Synopsis Record covering the period during which the ship was under their jurisdiction.

8 When a ship is transferred to the flag of another State the Government of which is a Contracting Government, the Contracting Government of the State whose flag the ship was flying hitherto shall transmit to the Administration as soon as possible after the transfer takes place a copy of the relevant Continuous Synopsis Record covering the period during which the ship was under their jurisdiction together with any Continuous Synopsis Records previously issued to the ship by other States.

9 When a ship is transferred to the flag of another State, the Administration shall append the previous Continuous Synopsis Records to the Continuous Synopsis Record the Administration will issue to the ship so to provide the continuous history record intended by this regulation.

10 The Continuous Synopsis Record shall be kept on board the ship and shall be available for inspection at all times."

7 The following new chapter XI-2 is inserted after the renumbered chapter XI-1:

**“CHAPTER XI-2
SPECIAL MEASURES TO ENHANCE MARITIME SECURITY**

**Regulation 1
Definitions**

1 For the purpose of this chapter, unless expressly provided otherwise:

- .1 *Bulk carrier* means a bulk carrier as defined in regulation IX/1.6.
- .2 *Chemical tanker* means a chemical tanker as defined in regulation VII/8.2.
- .3 *Gas carrier* means a gas carrier as defined in regulation VII/11.2.
- .4 *High-speed craft* means a craft as defined in regulation X/1.2.
- .5 *Mobile offshore drilling unit* means a mechanically propelled mobile offshore drilling unit, as defined in regulation IX/1, not on location.
- .6 *Oil tanker* means an oil tanker as defined in regulation II-1/2.12.
- .7 *Company* means a Company as defined in regulation IX/1.
- .8 *Ship/port interface* means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship.
- .9 *Port facility* is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.
- .10 *Ship to ship activity* means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.
- .11 *Designated Authority* means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.
- .12 *International Ship and Port Facility Security (ISPS) Code* means the International Code for the Security of Ships and of Port Facilities consisting of Part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International

Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization, provided that:

.1 amendments to part A of the Code are adopted, brought into force and take effect in accordance with article VIII of the present Convention concerning the amendment procedures applicable to the Annex other than chapter I; and

.2 amendments to part B of the Code are adopted by the Maritime Safety Committee in accordance with its Rules of Procedure.

.13 *Security incident* means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity.

.14 *Security level* means the qualification of the degree of risk that a security incident will be attempted or will occur.

.15 *Declaration of security* means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.

.16 *Recognized security organization* means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by this chapter or by part A of the ISPS Code.

2 The term "ship", when used in regulations 3 to 13, includes mobile offshore drilling units and high-speed craft.

3 The term "all ships", when used in this chapter, means any ship to which this chapter applies.

4 The term "Contracting Government", when used in regulations 3, 4, 7, 10, 11, 12 and 13 includes a reference to the "Designated Authority".

Regulation 2 Application

1 This chapter applies to:

.1 the following types of ships engaged on international voyages:

.1.1 passenger ships, including high-speed passenger craft;

.1.2 cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and

.1.3 mobile offshore drilling units; and

.2 port facilities serving such ships engaged on international voyages.

Notwithstanding the provisions of paragraph 1.2, Contracting Governments shall decide the extent of application of this chapter and of the relevant sections of part A of the ISPS Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

2.1 Contracting Governments shall base their decisions, under paragraph 2, on a port facility security assessment carried out in accordance with the provisions of part A of the ISPS Code.

2.2 Any decision which a Contracting Government makes, under paragraph 2, shall not compromise the level of security intended to be achieved by this chapter or by part A of the ISPS Code.

3 This chapter does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

4 Nothing in this chapter shall prejudice the rights or obligations of States under international law.

Regulation 3

Obligations of Contracting Governments with respect to security

1 Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag. When changes in security level occur, security level information shall be updated as the circumstance dictates.

2 Contracting Governments shall set security levels and ensure the provision of security level information to port facilities within their territory, and to ships prior to entering a port or whilst in a port within their territory. When changes in security level occur, security level information shall be updated as the circumstance dictates.

Regulation 4

Requirements for Companies and ships

1 Companies shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

2 Ships shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code, and such compliance shall be verified and certified as provided for in part A of the ISPS Code.

3 Prior to entering a port or whilst in a port within the territory of a Contracting Government, a ship shall comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship.

4 Ships shall respond without undue delay to any change to a higher security level.

5 Where a ship is not in compliance with the requirements of this chapter or of part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

Regulation 5

Specific responsibility of Companies

The Company shall ensure that the master has available on board, at all times, information through which officers duly authorised by a Contracting Government can establish:

- .1 who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;
- .2 who is responsible for deciding the employment of the ship; and
- .3 in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

Regulation 6

Ship security alert system

1 All ships shall be provided with a ship security alert system, as follows:

- .1 ships constructed on or after 1 July 2004;
- .2 passenger ships, including high-speed passenger craft, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;

.3 oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004; and

.4 other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.

2 The ship security alert system, when activated, shall:

.1 initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;

.2 not send the ship security alert to any other ships;

.3 not raise any alarm on-board the ship; and

.4 continue the ship security alert until deactivated and/or reset.

3 The ship security alert system shall:

.1 be capable of being activated from the navigation bridge and in at least one other location; and

.2 conform to performance standards not inferior to those adopted by the Organization.

4 The ship security alert system activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert.

5 The requirement for a ship security alert system may be complied with by using the radio installation fitted for compliance with the requirements of chapter IV, provided all requirements of this regulation are complied with.

6 When an Administration receives notification of a ship security alert, that Administration shall immediately notify the State(s) in the vicinity of which the ship is presently operating.

7 When a Contracting Government receives notification of a ship security alert from a ship which is not entitled to fly its flag, that Contracting Government shall immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

Regulation 7

Threats to ships

1 Contracting Governments shall set security levels and ensure the provision of security level information to ships operating in their territorial sea or having communicated an intention to enter their territorial sea.

2 Contracting Governments shall provide a point of contact through which such ships can request advice or assistance and to which such ships can report any security concerns about other ships, movements or communications.

3 Where a risk of attack has been identified, the Contracting Government concerned shall advise the ships concerned and their Administrations of:

.1 the current security level;

.2 any security measures that should be put in place by the ships concerned to protect themselves from attack, in accordance with the provisions of part A of the ISPS Code; and

.3 security measures that the coastal State has decided to put in place, as appropriate.

Regulation 8

Master's discretion for ship safety and security

1 The master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgement of the master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

2 If, in the professional judgement of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship. In such cases, the master may implement temporary security measures and shall forthwith inform the Administration and, if appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures under this regulation shall, to the highest possible degree, be commensurate with the prevailing security level. When such cases are identified, the Administration shall ensure that such conflicts are resolved and that the possibility of recurrence is minimised.

Regulation 9

Control and compliance measures

1 Control of ships in port

1.1 For the purpose of this chapter, every ship to which this chapter applies is subject to control when in a port of another Contracting Government by officers duly authorised by that Government, who may be the same as those carrying out the functions of regulation I/19. Such control shall be limited to verifying that there is onboard a valid International Ship Security Certificate or a valid Interim International Ships Security Certificate issued under the provisions of part A of the ISPS Code (Certificate), which if valid shall be accepted, unless there are clear grounds for believing that the ship is not in compliance with the requirements of this chapter or part A of the ISPS Code.

1.2 When there are such clear grounds, or where no valid Certificate is produced when required, the officers duly authorized by the Contracting Government shall impose any one or more control measures in relation to that ship as provided in paragraph 1.3. Any such measures imposed must be proportionate, taking into account the guidance given in part B of the ISPS Code.

Such control measures are as follows: inspection of the ship, delaying the ship, detention of the ship, restriction of operations including movement within the port, or expulsion of the ship from port. Such control measures may additionally or alternatively include other lesser administrative or corrective measures.

2 Ships intending to enter a port of another Contracting Government

2.1 For the purpose of this chapter, a Contracting Government may require that ships intending to enter its ports provide the following information to officers duly authorized by that Government to ensure compliance with this chapter prior to entry into port with the aim of avoiding the need to impose control measures or steps:

- .1 that the ship possesses a valid Certificate and the name of its issuing authority;
- .2 the security level at which the ship is currently operating;
- .3 the security level at which the ship operated in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;
- .4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;
- .5 that the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified in paragraph 2.3; or

.6 other practical security related information (but not details of the ship security plan), taking into account the guidance given in part B of the ISPS Code.

If requested by the Contracting Government, the ship or the Company shall provide confirmation, acceptable to that Contracting Government, of the information required above.

2.2 Every ship to which this chapter applies intending to enter the port of another Contracting Government shall provide the information described in paragraph 2.1 on the request of the officers duly authorized by that Government. The master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

2.3 The ship shall keep records of the information referred to in paragraph 2.1 for the last 10 calls at port facilities.

2.4 If, after receipt of the information described in paragraph 2.1, officers duly authorised by the Contracting Government of the port in which the ship intends to enter have clear grounds for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers shall attempt to establish communication with and between the ship and the Administration in order to rectify the non-compliance. If such communication does not result in rectification, or if such officers have clear grounds otherwise for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers may take steps in relation to that ship as provided in paragraph 2.5. Any such steps taken must be proportionate, taking into account the guidance given in part B of the ISPS Code.

2.5 Such steps are as follows:

- .1 a requirement for the rectification of the non-compliance;
- .2 a requirement that the ship proceed to a location specified in the territorial sea or internal waters of that Contracting Government;
- .3 inspection of the ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter; or
- .4 denial of entry into port.

Prior to initiating any such steps, the ship shall be informed by the Contracting Government of its intentions. Upon this information the master may withdraw the intention to enter that port. In such cases, this regulation shall not apply.

3 Additional provisions

3.1 In the event:

.1 of the imposition of a control measure, other than a lesser administrative or corrective measure, referred to in paragraph 1.3; or

.2 any of the steps referred to in paragraph 2.5 are taken,

an officer duly authorized by the Contracting Government shall forthwith inform in writing the Administration specifying which control measures have been imposed or steps taken and the reasons thereof. The Contracting Government imposing the control measures or steps shall also notify the recognized security organization, which issued the Certificate relating to the ship concerned and the Organization when any such control measures have been imposed or steps taken.

3.2 When entry into port is denied or the ship is expelled from port, the authorities of the port State should communicate the appropriate facts to the authorities of the State of the next appropriate ports of call, when known, and any other appropriate coastal States, taking into account guidelines to be developed by the Organization. Confidentiality and security of such notification shall be ensured.

3.3 Denial of entry into port, pursuant to paragraphs 2.4 and 2.5, or expulsion from port, pursuant to paragraphs 1.1 to 1.3, shall only be imposed where the officers duly authorized by the Contracting Government have clear grounds to believe that the ship poses an immediate threat to the security or safety of persons, or of ships or other property and there are no other appropriate means for removing that threat.

3.4 The control measures referred to in paragraph 1.3 and the steps referred to in paragraph 2.5 shall only be imposed, pursuant to this regulation, until the non-compliance giving rise to the control measures or steps has been corrected to the satisfaction of the Contracting Government, taking into account actions proposed by the ship or the Administration, if any.

3.5 When Contracting Governments exercise control under paragraph 1 or take steps under paragraph 2:

.1 all possible efforts shall be made to avoid a ship being unduly detained or delayed. If a ship is thereby unduly detained, or delayed, it shall be entitled to compensation for any loss or damage suffered; and

.2 necessary access to the ship shall not be prevented for emergency or humanitarian reasons and for security purposes.

Regulation 10

Requirements for port facilities

Port facilities shall comply with the relevant requirements of this chapter and part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

2 Contracting Governments with a port facility or port facilities within their territory, to which this regulation applies, shall ensure that:

.1 port facility security assessments are carried out, reviewed and approved in accordance with the provisions of part A of the ISPS Code; and

.2 port facility security plans are developed, reviewed, approved and implemented in accordance with the provisions of part A of the ISPS Code.

3 Contracting Governments shall designate and communicate the measures required to be addressed in a port facility security plan for the various security levels, including when the submission of a Declaration of Security will be required.

Regulation 11

Alternative security agreements

1 Contracting Governments may, when implementing this chapter and part A of the ISPS Code, conclude in writing bilateral or multilateral agreements with other Contracting Governments on alternative security arrangements covering short international voyages on fixed routes between port facilities located within their territories.

2 Any such agreement shall not compromise the level of security of other ships or of port facilities not covered by the agreement.

3 No ship covered by such an agreement shall conduct any ship-to-ship activities with any ship not covered by the agreement.

4 Such agreements shall be reviewed periodically, taking into account the experience gained as well as any changes in the particular circumstances or the assessed threats to the security of the ships, the port facilities or the routes covered by the agreement.

Regulation 12

Equivalent security arrangements

1 An Administration may allow a particular ship or a group of ships entitled to fly its flag to implement other security measures equivalent to those prescribed in this chapter or in part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Administration, which

allows such security measures, shall communicate to the Organization particulars thereof.

2 When implementing this chapter and part A of the ISPS Code, a Contracting Government may allow a particular port facility or a group of port facilities located within its territory, other than those covered by an agreement concluded under regulation 11, to implement security measures equivalent to those prescribed in this chapter or in Part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Contracting Government, which allows such security measures, shall communicate to the Organization particulars thereof.

Regulation 13

Communication of information

1 Contracting Governments shall, not later than 1 July 2004, communicate to the Organization and shall make available for the information of Companies and ships:

- .1 the names and contact details of their national authority or authorities responsible for ship and port facility security;
- .2 the locations within their territory covered by the approved port facility security plans.
- .3 the names and contact details of those who have been designated to be available at all times to receive and act upon the ship-to-shore security alerts, referred to in regulation 6.2.1;
- .4 the names and contact details of those who have been designated to be available at all times to receive and act upon any communications from Contracting Governments exercising control and compliance measures, referred to in regulation 9.3.1; and
- .5 the names and contact details of those who have been designated to be available at all times to provide advice or assistance to ships and to whom ships can report any security concerns, referred to in regulation 7.2;

and thereafter update such information as and when changes relating thereto occur. The Organization shall circulate such particulars to other Contracting Governments for the information of their officers.

2 Contracting Governments shall, not later than 1 July 2004, communicate to the Organization the names and contact details of any recognized security organizations authorized to act on their behalf together with details of the specific responsibility and conditions of authority delegated to such organizations. Such information shall be

updated as and when changes relating thereto occur. The Organization shall circulate such particulars to other Contracting Governments for the information of their officers.

3 Contracting Governments shall, not later than 1 July 2004 communicate to the Organization a list showing the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval and thereafter shall further communicate when any of the following changes take place:

.1 changes in the location or locations covered by an approved port facility security plan are to be introduced or have been introduced. In such cases the information to be communicated shall indicate the changes in the location or locations covered by the plan and the date as of which such changes are to be introduced or were implemented;

.2 an approved port facility security plan, previously included in the list submitted to the Organization, is to be withdrawn or has been withdrawn. In such cases, the information to be communicated shall indicate the date on which the withdrawal will take effect or was implemented. In these cases, the communication shall be made to the Organization as soon as is practically possible; and

.3 additions are to be made to the list of approved port facility security plans. In such cases, the information to be communicated shall indicate the location or locations covered by the plan and the date of approval.

4 Contracting Governments shall, at five year intervals after 1 July 2004, communicate to the Organization a revised and updated list showing all the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval (and the date of approval of any amendments thereto) which will supersede and replace all information communicated to the Organization, pursuant to paragraph 3, during the preceding five years.

5 Contracting Governments shall communicate to the Organization information that an agreement under regulation 11 has been concluded. The information communicated shall include:

.1 the names of the Contracting Governments which have concluded the agreement;

.2 the port facilities and the fixed routes covered by the agreement;

.3 the periodicity of review of the agreement;

.4 the date of entry into force of the agreement; and

.5 information on any consultations which have taken place with other Contracting Governments;

and thereafter shall communicate, as soon as practically possible, to the Organization information when the agreement has been amended or has ended.

6 Any Contracting Government which allows, under the provisions of regulation 12, any equivalent security arrangements with respect to a ship entitled to fly its flag or with respect to a port facility located within its territory, shall communicate to the Organization particulars thereof.

7 The Organization shall make available the information communicated under paragraph 3 to other Contracting Governments upon request.

Article 3.

The execution of this Decree is in the competence of the Ministry of Maritime Affairs, Traffic and Communications.

Article 4.

The International Code for the Security of Ships and of Port Facilities (ISPS) referred to in the Chapter XI-2 of the Amendments set forth in Article 2. of this Decree in the original copy in English language and in translation into Croatian language shall be published in "Narodne Novine" by the competent Ministry and shall enter into force together with the entry into force of the Amendments set forth in Article 2.

Article 5.

This Decree shall enter into force on the 8th day from its publication in "Narodne Novine". The Amendments set forth in Article 2. of this Decree shall not be in force on the day of entry into force of this Decree. The information about their entry into force shall be subsequently announced in accordance with article 30. paragraph 3. of the Law on Conclusion and Execution of International Agreements ("Narodne Novine" No. 28/96) after their entry into force.

Class: XXX-XX/XX-XX/XX
Reg. Number: XXXXXXX-XX-X
Zagreb, dd.mm.yyyy.

The Premier

THE MINISTRY OF MARITIME AFFAIRS, TRAFFIC AND COMMUNICATIONS OF THE REPUBLIC OF CROATIA

On the basis of Articles 3. and 4. of the Decree publishing the Amendments to the Annex to the Convention for the Safety of Life at Sea ("Narodne Novine" – International Agreements No. XX/YY), the Minister of Maritime Affairs, Traffic and Communications publishes The International Code for the Security of Ships and of Port Facilities (ISPS), which upon its entry into force shall form an integral part of the 1974 Convention for the Safety of Life at Sea, and which in the original English language copy and the translation into Croatian language reads as follows:

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES

PREAMBLE

1. The Diplomatic Conference on Maritime Security held in London in December 2002 adopted new provisions in the International Convention for the Safety of Life at Sea, 1974 and this Code* to enhance maritime security. These new requirements form the international framework through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

2. Following the tragic events of 11th September 2001, the twenty-second session of the Assembly of the International Maritime Organization (the Organization), in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (known as the Diplomatic Conference on Maritime Security) in December 2002. Preparation for the Diplomatic Conference was entrusted to the Organization's Maritime Safety Committee (MSC) on the basis of submissions made by Member States, intergovernmental

* The complete name of this Code is the International Code for the Security of Ships and of Port Facilities. The abbreviated name of this Code, as referred to in regulation XI-2/1 of SOLAS 74 as amended, is the International Ship and Port Facility Security (ISPS) Code or, in short, the ISPS Code.

organizations and non-governmental organizations in consultative status with the Organization.

3. The MSC, at its first extraordinary session, held also in November 2001, in order to accelerate the development and the adoption of the appropriate security measures established an MSC Intersessional Working Group on Maritime Security. The first meeting of the MSC Intersessional Working Group on Maritime Security was held in February 2002 and the outcome of its discussions was reported to, and considered by, the seventy-fifth session of the MSC in March 2002, when an *ad hoc* Working Group was established to further develop the proposals made. The seventy-fifth session of the MSC considered the report of that Working Group and recommended that work should be taken forward through a further MSC Intersessional Working Group, which was held in September 2002. The seventy-sixth session of the MSC considered the outcome of the September 2002 session of the MSC Intersessional Working Group and the further work undertaken by the MSC Working Group held in conjunction with the Committee's seventy-sixth session in December 2002, immediately prior to the Diplomatic Conference and agreed the final version of the proposed texts to be considered by the Diplomatic Conference.

4. The Diplomatic Conference (9 to 13 December 2002) also adopted amendments to the existing provisions of the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) accelerating the implementation of the requirement to fit Automatic Identification Systems and adopted new Regulations in Chapter XI-1 of SOLAS 74 covering marking of the Ship's Identification Number and the carriage of a Continuous Synopsis Record. The Diplomatic Conference also adopted a number of Conference Resolutions including those covering implementation and revision of this Code, Technical Co-operation, and co-operative work with the International Labour Organization and World Customs Organization. It was recognized that review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these two Organizations.

5. The provision of Chapter XI-2 of SOLAS 74 and this Code apply to ships and to port facilities. The extension of SOLAS 74 to cover port facilities was agreed on the basis that SOLAS 74 offered the speediest means of ensuring the necessary security measures entered into force and given effect quickly. However, it was further agreed that the provisions relating to port facilities should relate solely to the ship/port interface. The wider issue of the security of port areas will be the subject of further joint work between the International Maritime Organization and the International Labour Organization. It was also agreed that the provisions should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack.

6. In drafting the provision care has been taken to ensure compatibility with the provisions of the International Convention on Standards of Training, Certification and Watchkeeping and Certification for Seafarers, 1978, as amended, the International Safety Management (ISM) Code and the harmonised system of survey and certification.

7. The provisions represent a significant change in the approach of the international maritime industries to the issue of security in the maritime transport sector. It is recognized that they may place a significant additional burden on certain Contracting Governments. The importance of Technical Co-operation to assist Contracting Governments implement the provisions is fully recognized.

8. Implementation of the provisions will require continuing effective co-operation and understanding between all those involved with, or using, ships and port facilities including ship's personnel, port personnel, passengers, cargo interests, ship and port management and those in National and Local Authorities with security responsibilities. Existing practices and procedures will have to be reviewed and changed if they do not provide an adequate level of security. In the interests of enhanced maritime security additional responsibilities will have to be carried by the shipping and port industries and by National and Local Authorities.

9. The guidance given in part B of this Code should be taken into account when implementing the security provisions set out in Chapter XI-2 of SOLAS 74 and in part A of this Code. However, it is recognized that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/or cargo.

10. Nothing in this Code shall be interpreted or applied in a manner inconsistent with the proper respect of fundamental rights and freedoms as set out in international instruments, particularly those relating to maritime workers and refugees including the International Labour Organization Declaration of Fundamental Principles and Rights at Work as well as international standards concerning maritime and port workers.

11. Recognizing that the Convention on the Facilitation of Maritime Traffic, 1965, as amended, provides that foreign crew members shall be allowed ashore by the public authorities while the ship on which they arrive is in port, provided that the formalities on arrival of the ship have been fulfilled and the public authorities have no reason to refuse permission to come ashore for reasons of public health, public safety or public order, Contracting Governments when approving ship and port facility security plans should pay due cognisance to the fact that ship's personnel live and work on the vessel and need shore leave and access to shore based seafarer welfare facilities, including medical care.

PART A

MANDATORY REQUIREMENTS REGARDING THE PROVISIONS OF CHAPTER XI-2 OF THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974, AS AMENDED

1 GENERAL

1.1 Introduction

This part of the International Code for the Security of Ships and Port Facilities contains mandatory provisions to which reference is made in chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974 as amended.

1.2 Objectives

The objectives of this Code are:

- .1 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;
- .2 to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security;
- .3 to ensure the early and efficient collection and exchange of security-related information;
- .4 to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
- .5 to ensure confidence that adequate and proportionate maritime security measures are in place.

1.3 Functional requirements

In order to achieve its objectives, this Code embodies a number of functional requirements. These include, but are not limited to:

- .1 gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
- .2 requiring the maintenance of communication protocols for ships and port facilities;
- .3 preventing unauthorized access to ships, port facilities and their restricted areas;
- .4 preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;
- .5 providing means for raising the alarm in reaction to security threats or security incidents;
- .6 requiring ship and port facility security plans based upon security assessments; and
- .7 requiring training, drills and exercises to ensure familiarity with security plans and procedures.

2 DEFINITIONS

2.1 For the purpose of this part, unless expressly provided otherwise:

- .1 *Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.
- .2 *Regulation* means a regulation of the Convention.
- .3 *Chapter* means a chapter of the Convention.
- .4 *Ship security plan* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

- .5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.
- .6 *Ship security officer* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.
- .7 *Company security officer* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.
- .8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.
- .9 *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times.
- .10 *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- .11 *Security level 3* means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.2 The term "ship", when used in this Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term "Contracting Government" in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the "Designated Authority".

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

3 APPLICATION

3.1 This Code applies to:

- .1 the following types of ships engaged on international voyages:
 - .1 passenger ships, including high-speed passenger craft;
 - .2 cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and
 - .3 mobile offshore drilling units; and
- .2 port facilities serving such ships engaged on international voyages.

3.2 Notwithstanding the provisions of section 3.1.2, Contracting Governments shall decide the extent of application of this Part of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

3.2.1 Contracting Governments shall base their decisions, under section 3.2, on a port facility security assessment carried out in accordance with this Part of the Code.

3.2.2 Any decision which a Contracting Government makes, under section 3.2, shall not compromise the level of security intended to be achieved by chapter XI-2 or by this Part of the Code.

3.3 This Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

3.4 Sections 5 to 13 and 19 of this part apply to Companies and ships as specified in regulation XI-2/4.

3.5 Sections 5 and 14 to 18 of this part apply to port facilities as specified in regulation XI-2/10.

3.6 Nothing in this Code shall prejudice the rights or obligations of States under international law.

4 *RESPONSIBILITIES OF CONTRACTING GOVERNMENTS*

4.1 Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

- .1 the degree that the threat information is credible;
- .2 the degree that the threat information is corroborated;
- .3 the degree that the threat information is specific or imminent; and
- .4 the potential consequences of such a security incident.

4.2 Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

4.3 Contracting Governments may delegate to a recognized security organization certain of their security related duties under chapter XI-2 and this Part of the Code with the exception of:

- .1 setting of the applicable security level;
- .2 approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;
- .3 determining the port facilities which will be required to designate a Port Facility Security Officer;
- .4 approving a Port Facility Security Plan and subsequent amendments to an approved plan;
- .5 exercising control and compliance measures pursuant to regulation XI-2/9; and
- .6 establishing the requirements for a Declaration of Security.

4.4 Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

5 DECLARATION OF SECURITY

5.1 Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses to persons, property or the environment.

5.2 A ship can request completion of a Declaration of Security when:

- .1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;
- .2 there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
- .3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
- .4 the ship is at a port which is not required to have and implement an approved port facility security plan; or
- .5 the ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.

5.3 Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.

5.4 The Declaration of Security shall be completed by:

- .1 the master or the ship security officer on behalf of the ship(s); and, if appropriate,
- .2 the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

5.5 The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

5.6 Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

5.7 Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

6 OBLIGATIONS OF THE COMPANY

6.1 The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

6.2 The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this Part of the Code.

7 SHIP SECURITY

7.1 A ship is required to act upon the security levels set by Contracting Governments as set out below.

7.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

- .1 ensuring the performance of all ship security duties;

- .2 controlling access to the ship;
- .3 controlling the embarkation of persons and their effects;
- .4 monitoring restricted areas to ensure that only authorized persons have access;
- .5 monitoring of deck areas and areas surrounding the ship;
- .6 supervising the handling of cargo and ship's stores; and
- .7 ensuring that security communication is readily available.

7.3 At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.4 At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.5 Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

7.6 Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

7.7 If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

7.7.1 In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

7.8 An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

7.9 When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

7.9.1 When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in the part B of this Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

8 SHIP SECURITY ASSESSMENT

8.1 The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

8.2 The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this section, taking into account the guidance given in part B of this Code.

8.3 Subject to the provisions of section 9.2.1, a recognized security organization may carry out the ship security assessment of a specific ship.

8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

- .1 identification of existing security measures, procedures and operations;
- .2 identification and evaluation of key ship board operations that it is important to protect;
- .3 identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and
- .4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

8.5 The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

9.1 Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in this Part of the Code.

9.1.1 Subject to the provisions of section 9.2.1, a recognized security organization may prepare the ship security plan for a specific ship.

9.2 The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations.

9.2.1 In such cases the recognized security organization, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

9.3 The submission of a ship security plan, or of amendments to a previously approved plan, for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, have been developed.

9.4 Such a plan shall be developed, taking into account the guidance given in part B of this Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

- .1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;**
- .2 identification of the restricted areas and measures for the prevention of unauthorized access to them;**
- .3 measures for the prevention of unauthorized access to the ship;
- .4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;**
- .5 procedures for responding to any security instructions Contracting Governments may give at security level 3;**

- .6 procedures for evacuation in case of security threats or breaches of security;**
- .7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;**
- .8 procedures for auditing the security activities;**
- .9 procedures for training, drills and exercises associated with the plan;**
- .10 procedures for interfacing with port facility security activities;**
- .11 procedures for the periodic review of the plan and for updating;**
- .12 procedures for reporting security incidents;**
- .13 identification of the ship security officer;**
- .14 identification of the company security officer including 24-hour contact details;**
- .15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;**
- .16 frequency for testing or calibration of any security equipment provided on board;**
- .17 identification of the locations where the ship security alert system activation points are provided;¹ and**
- .18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.¹**

¹ Administrations may allow, in order to avoid compromising in any way the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

9.5 The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this Part of the Code.

9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

9.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

9.7 The plan shall be protected from unauthorized access or disclosure.

9.8 Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9, save in circumstances specified in section 9.8.1.

9.8.1 If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this Part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

10.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

- .1 training, drills and exercises;
- .2 security threats and security incidents;
- .3 breaches of security;
- .4 changes in security level;
- .5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- .6 internal audits and reviews of security activities;
- .7 periodic review of the ship security assessment;
- .8 periodic review of the ship security plan;
- .9 implementation of any amendments to the plan; and
- .10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

10.2 The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

10.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment.

10.4 The records shall be protected from unauthorized access or disclosure.

11 COMPANY SECURITY OFFICER

11.1 The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

11.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

- .1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- .2 ensuring that ship security assessments are carried out;
- .3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- .4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- .5 arranging for internal audits and reviews of security activities;
- .6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;
- .7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
- .8 enhancing security awareness and vigilance;
- .9 ensuring adequate training for personnel responsible for the security of the ship;
- .10 ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;
- .11 ensuring consistency between security requirements and safety requirements;
- .12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- .13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

12 SHIP SECURITY OFFICER

12.1 A ship security officer shall be designated on each ship.

12.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

- .1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- .2 maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
- .3 co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
- .4 proposing modifications to the ship security plan;
- .5 reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
- .6 enhancing security awareness and vigilance on board;
- .7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;
- .8 reporting all security incidents;
- .9 co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and
- .10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

13.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.3 Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan

and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

13.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.

13.5 The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

14 PORT FACILITY SECURITY

14.1 A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

14.2 At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

- .1 ensuring the performance of all port facility security duties;
- .2 controlling access to the port facility;
- .3 monitoring of the port facility, including anchoring and berthing area(s);
- .4 monitoring restricted areas to ensure that only authorized persons have access;
- .5 supervising the handling of cargo;
- .6 supervising the handling of ship's stores; and
- .7 ensuring that security communication is readily available.

14.3 At security level 2, the additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4 At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4.1 In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.

14.5 When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security officer and ship security officer shall liaise and co-ordinate appropriate actions.

14.6 When a port facility security officer is advised that a ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

15 PORT FACILITY SECURITY ASSESSMENT

15.1 The port facility security assessment is an essential and integral part of the process of developing and updating the port facility security plan.

15.2 The port facility security assessment shall be carried out by the Contracting Government within whose territory the port facility is located. A Contracting Government may authorise a recognized security organization to carry out the port facility security assessment of a specific port facility located within its territory.

15.2.1 When the port facility security assessment has been carried out by a recognized security organization, the security assessment shall be reviewed and approved for compliance with this section by the Contracting Government within whose territory the port facility is located.

15.3 The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, taking into account the guidance given in part B of this Code.

15.4 The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

15.5 The port facility security assessment shall include, at least, the following elements:

- .1 identification and evaluation of important assets and infrastructure it is important to protect;
- .2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;
- .3 identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and
- .4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

15.6 The Contracting Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an arrangement shall communicate to the Organization particulars thereof.

15.7 Upon completion of the port facility security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

16 PORT FACILITY SECURITY PLAN

16.1 A port facility security plan shall be developed and maintained, on the basis of a port facility security assessment, for each port facility, adequate for the ship/port interface. The plan shall make provisions for the three security levels, as defined in this Part of the Code.

16.1.1 Subject to the provisions of section 16.2, a recognized security organization may prepare the port facility security plan of a specific port facility.

16.2 The port facility security plan shall be approved by the Contracting Government in whose territory the port facility is located.

16.3 Such a plan shall be developed taking into account the guidance given in part B of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

- .1 measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;
 - .2 measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;
 - .3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/ port interface;
 - .4 procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3;**
 - .5 procedures for evacuation in case of security threats or breaches of security;
 - .6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;
 - .7 procedures for interfacing with ship security activities;
 - .8 procedures for the periodic review of the plan and updating;
 - .9 procedures for reporting security incidents;
 - .10 identification of the port facility security officer including 24-hour contact details;**
 - .11 measures to ensure the security of the information contained in the plan;
 - .12 measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;
 - .13 procedures for auditing the port facility security plan;
 - .14 procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

- .15 procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organizations.

16.3.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

16.4 The port facility security plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans.

16.5 The Contracting Government in whose territory the port facility is located shall determine which changes to the port facility security plan shall not be implemented unless the relevant amendments to the plan are approved by them.

16.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

16.7 The plan shall be protected from unauthorized access or disclosure.

16.8 Contracting Governments may allow a port facility security plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an alternative arrangement, shall communicate to the Organization particulars thereof.

17 PORT FACILITY SECURITY OFFICER

17.1 A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

17.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

- .1 conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
- .2 ensuring the development and maintenance of the port facility security plan;
- .3 implementing and exercising the port facility security plan;

- .4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
- .5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
- .6 enhancing security awareness and vigilance of the port facility personnel;
- .7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- .8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- .9 co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- .10 co-ordinating with security services, as appropriate;
- .11 ensuring that standards for personnel responsible for security of the port facility are met;
- .12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
- .13 assisting ship security officers in confirming the identity of those seeking to board the ship when requested.**

17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and this Part of the Code.

18 TRAINING, DRILLS AND EXERCISES ON PORT FACILITY SECURITY

18.1 The port facility security officer and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

18.2 Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the port facility

security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

18.3 To ensure the effective implementation of the port facility security plan, drills shall be carried out at appropriate intervals taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in part B of this Code.

18.4 The port facility security officer shall ensure the effective coordination and implementation of the port facility security plan by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

19 Verification and certification for ships

19.1 Verifications

19.1.1 Each ship to which this Part of the Code applies shall be subject to the verifications specified below:

- .1 an initial verification before the ship is put in service or before the certificate required under section 19.2 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of chapter XI-2, this Part of the Code and the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and this Part of the Code, is in satisfactory condition and fit for the service for which the ship is intended;
- .2 a renewal verification at intervals specified by the Administration, but not exceeding five years, except where section 19.3 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2, this Part of the Code and the approved ship security plan, is in satisfactory condition and fit for the service for which the ship is intended;
- .3 at least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second and third anniversary date of the certificate as defined in regulation I/2(n). The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;

.4 any additional verifications as determined by the Administration.

19.1.2 The verifications of ships shall be carried out by officers of the Administration. The Administration may, however, entrust the verifications to a recognized security organization referred to in regulation XI-2/1.

19.1.3 In every case, the Administration concerned shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

19.1.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, this Part of the Code and the approved ship security plan. After any verification under section 19.1.1 has been completed, no changes shall be made in security system and in any associated security equipment or the approved ship security plan without the sanction of the Administration.

19.2 Issue or endorsement of certificate

19.2.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

19.2.2 Such certificate shall be issued or endorsed either by the Administration or by a recognized security organization acting on behalf of the Administration.

19.2.3 Another Contracting Government may, at the request of the Administration, cause the ship to be verified and, if satisfied that the provisions of section 19.1.1 are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship and, where appropriate, endorse or authorize the endorsement of that certificate on the ship, in accordance with this Code.

19.2.3.1 A copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Administration.

19.2.3.2 A certificate so issued shall contain a statement to the effect that it has been issued at the request of the Administration and it shall have the same force and receive the same recognition as the certificate issued under section 19.2.2.

19.2.4 The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix to this Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

19.3 Duration and validity of certificate

19.3.1 An International Ship Security Certificate shall be issued for a period specified by the Administration which shall not exceed five years.

19.3.2 When the renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

19.3.2.1 When the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

19.3.2.2 When the renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

19.3.3 If a certificate is issued for a period of less than five years, the Administration may extend the validity of the certificate beyond the expiry date to the maximum period specified in section 19.3.1, provided that the verifications referred to in section 19.1.1 applicable when a certificate is issued for a period of five years are carried out as appropriate.

19.3.4 If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the Administration or recognized security organization acting on behalf of the Administration may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

19.3.5 If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Administration may extend the period of validity of the certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and then only in cases where it appears proper and reasonable to do so. No certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the expiry date of the existing certificate before the extension was granted.

19.3.6 A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the date of expiry of the existing certificate before the extension was granted.

19.3.7 If an intermediate verification is completed before the period specified in section

19.1.1, then:

- .1 the expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;
- .2 the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by section 19.1.1 are not exceeded.

19.3.8 A certificate issued under section 19.2 shall cease to be valid in any of the following cases:

- .1 if the relevant verifications are not completed within the periods specified under section 19.1.1;
- .2 if the certificate is not endorsed in accordance with section 19.1.1.3 and 19.3.7.1, if applicable;
- .3 when a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and
- .4 upon transfer of the ship to the flag of another State.

19.3.9 In the case of:

- .1 a transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports, or
- .2 a Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in section 19.4.2.

19.4 Interim certification

19.4.1 The certificates specified in section 19.2 shall be issued only when the Administration issuing the certificate is fully satisfied that the ship complies with the requirements of section 19.1. However, after 1 July 2004, for the purposes of:

- .1 a ship without a certificate, on delivery or prior to its entry or re-entry into service;

- .2 transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government;
- .3 transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government; or
- .4 when a Company assumes the responsibility for the operation of a ship not previously operated by that Company;

until the certificate referred to in section 19.2 is issued, the Administration may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the Appendix to this Part of the Code.

19.4.2 An Interim International Ship Security Certificate shall only be issued when the Administration or recognized security organization, on behalf of the Administration, has verified that:

- .1 the ship security assessment required by this Part of the Code has been completed,
- .2 a copy of the ship security plan meeting the requirements of chapter XI-2 and part A of this Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;
- .3 the ship is provided with a ship security alert system meeting the requirements of regulation XI-2/6, if required,
- .4 the company security officer:
 - .1 has ensured:
 - .1 the review of the ship security plan for compliance with this Part of the Code,
 - .2 that the plan has been submitted for approval, and
 - .3 that the plan is being implemented on the ship, and
 - .2 has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the company security officer is satisfied that the ship will successfully complete the required verification in accordance with section 19.1.1.1, within 6 months;

- .5 arrangements have been made for carrying out the required verifications under section 19.1.1.1;
- .6 the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this Part of the Code; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them; and
- .7 the ship security officer meets the requirements of this Part of the Code.

19.4.3 An Interim International Ship Security Certificate may be issued by the Administration or by a recognized security organization authorized to act on its behalf.

19.4.4 An Interim International Ship Security Certificate shall be valid for 6 months, or until the certificate required by section 19.2 is issued, whichever comes first, and may not be extended.

19.4.5 No Contracting Government shall cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgment of the Administration or the recognized security organization, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and this Part of the Code beyond the period of the initial interim certificate as specified in section 19.4.4.

19.4.6 For the purposes of regulation XI-2/9, Contracting Governments may, prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the requirements of sections 19.4.2.4 to 19.4.2.6 have been met.

APPENDIX TO PART A

APPENDIX 1

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal)

(State)

Certificate Number

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the Government of

_____ (name of State)

by _____
(persons or organization authorized)

Name of ship

.....

Distinctive number or letters

.....

Port of registry

.....

Type of ship

.....

Gross tonnage

.....

IMO Number

.....

Name and address of the Company

.....

THIS IS TO CERTIFY:

- 1 that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;
- 2 that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;
- 3 that the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based

.....

Date

.....

(Seal or stamp of the authority, as appropriate)

Additional verification

.....

official)

Signed

(Signature of authorized

Place

.....

Date

.....

(Seal or stamp of the authority, as appropriate)

Additional verification

.....

official)

Signed

(Signature of authorized

Place

.....

Date

.....

(Seal or stamp of the authority, as appropriate)

* This part of the certificate shall be adapted by the Administration to indicate whether it has established additional verifications as provided for in section 19.1.1.4.

**ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF
THE ISPS CODE**

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

.....
Signed
(Signature of authorized official)
Place
.....
Date
.....
(Seal or stamp of the authority, as appropriate)

**ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN
5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until

.....
Signed
(Signature of authorized official)
Place
.....
Date
.....
(Seal or stamp of the authority, as appropriate)

**ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN
COMPLETED AND SECTION A/19.3.4 OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until

.....
Signed
(Signature of authorized official)

Place

.....

Date

.....

(Seal or stamp of the authority, as appropriate)

**ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE
UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF
THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE
SECTION A/19.3.6 OF THE ISPS CODE APPLIES**

This Certificate shall, in accordance with section 19.3.5 / 19.3.6* of part A of the ISPS Code, be accepted as valid until

Signed

.....

(Signature of authorized official)

Place

.....

Date

.....

(Seal or stamp of the authority, as appropriate)

* Delete as appropriate.

**ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE
WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES**

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date** is
.....

.....

Signed

(Signature of authorized official)

.....

Place

.....

Date

(Seal or stamp of the authority, as appropriate)

** In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

APPENDIX 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal)

(State)

Certificate No.

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the Government of _____

(name of State)

by _____

(persons or organization authorized)

Name of ship :

Distinctive number or letters :

Port of registry :

Type of ship :

Gross tonnage :

IMO Number :

Name and address of company :

Is this a subsequent, consecutive interim certificate? Yes/ No*

If Yes, date of issue of initial interim certificate.....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until

Issued at

(place of issue of the certificate)

Date of issue

*(signature of the duly authorized official
issuing the Certificate)*

(Seal or stamp of issuing authority, as appropriate)

* Delete as appropriate

PART B

GUIDANCE REGARDING THE PROVISIONS OF
CHAPTER XI-2 OF THE ANNEX TO THE
INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 AS AMENDED
AND
PART A OF THIS CODE

1 INTRODUCTION

General

1.1 The preamble of this Code indicates that chapter XI-2 and part A of this Code establish the new international framework of measures to enhance maritime security and through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

1.2 This introduction outlines, in a concise manner, the processes envisaged in establishing and implementing the measures and arrangements needed to achieve and maintain compliance with the provisions of chapter XI-2 and of part A of this Code and identifies the main elements on which guidance is offered. The guidance is provided in paragraphs 2 through to 19. It also sets down essential considerations, which should be taken into account when considering the application of the guidance relating to ships and port facilities.

1.3 If the reader's interest relates to ships alone, it is strongly recommended that this Part of the Code is still read as a whole, particularly the sections relating to port facilities. The same applies to those whose primary interest are port facilities; they should also read the sections relating to ships.

1.4 The guidance provided in the following sections relates primarily to protection of the ship when it is at a port facility. There could, however, be situations when a ship may pose a threat to the port facility, e.g. because, once within the port facility, it could be used as a base from which to launch an attack. When considering the appropriate security measures to respond to ship-based security threats, those completing the Port Facility Security Assessment or preparing the Port Facility Security Plan should consider making appropriate adaptations to the guidance offered in the following sections.

1.5 The reader is advised that nothing in this Part of the Code should be read or interpreted in conflict with any of the provisions of either chapter XI-2 or part A of this Code and that the aforesaid provisions always prevail and override any unintended inconsistency which may have been inadvertently expressed in this Part of the Code. The guidance provided in this Part of the Code should always be read, interpreted and

applied in a manner which is consistent with the aims, objectives and principles established in chapter XI-2 and part A of this Code.

Responsibilities of Contracting Governments

1.6 Contracting Governments have, under the provisions of chapter XI-2 and part A of this Code, various responsibilities, which, amongst others, include:

- setting the applicable security level;
- approving the Ship Security Plan and relevant amendments to a previously approved plan;
- verifying the compliance of ships with the provisions of chapter XI-2 and part A of this Code and issuing to ships the International Ship Security Certificate;
- determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port Facility Security Plan;
- ensuring completion and approval of the Port Facility Security Assessment and of any subsequent amendments to a previously approved assessment;
- approving the Port Facility Security Plan and any subsequent amendments to a previously approved plan; and
- exercising control and compliance measures;
- testing approved plans; and
- communicating information to the International Maritime Organization and to the shipping and port industries.

1.7 Contracting Governments can designate, or establish, Designated Authorities within Government to undertake, with respect to port facilities, their security duties under chapter XI-2 and part A of this Code and allow Recognized Security Organizations to carry out certain work with respect to port facilities but the final decision on the acceptance and approval of this work should be given by the Contracting Government or the Designated Authority. Administrations may also delegate the undertaking of certain security duties, relating to ships, to Recognized Security Organizations. The following duties or activities cannot be delegated to a Recognized Security Organization:

- setting of the applicable security level;

- determining which of the port facilities located within the territory of a Contracting Government are required to designate a Port Facility Security Officer and to prepare a Port Facility Security Plan;
- approving a Port Facility Security Assessment or any subsequent amendments to a previously approved assessment;
- approving a Port Facility Security Plan or any subsequent amendments to a previously approved plan;
- exercising control and compliance measures; and
- establishing the requirements for a Declaration of Security.

Setting the security level

1.8 The setting of the security level applying at any particular time is the responsibility of Contracting Governments and can apply to ships and port facilities. Part A of this Code defines three security levels for international use. These are:

- Security Level 1, normal; the level at which ships and port facilities normally operate;
- Security Level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and
- Security Level 3, exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

The Company and the Ship

1.9 Any Company operating ships to which chapter XI-2 and part A of this Code apply has to designate a Company Security Officer for the Company and a Ship Security Officer for each of its ships. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.10 The Company Security Officer's responsibilities include, in brief amongst others, ensuring that a Ship Security Assessment is properly carried out, that a Ship Security Plan is prepared and submitted for approval by, or on behalf of, the Administration and thereafter is placed on board each ship to which part A of this Code applies and in respect of which that person has been appointed as the Company Security Officer.

1.11 The Ship Security Plan should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.

1.12 The ships to which the requirements of chapter XI-2 and part A of this Code apply are required to have, and operated in accordance with, a Ship Security Plan approved by, or on behalf of, the Administration. The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan, for which the Administration has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation by the ship.

1.13 The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of this Code. Part A of this Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

1.14 When a ship is at a port or is proceeding to a port of a Contracting Government, the Contracting Government has the right, under the provisions of regulation XI-2/9, to exercise various control and compliance measures with respect to that ship. The ship is subject to port State control inspections but such inspections will not normally extend to examination of the Ship Security Plan itself except in specific circumstances. The ship may, also, be subject to additional control measures if the Contracting Government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

1.15 The ship is also required to have onboard information, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship.

The port facility

1.16 Each Contracting Government has to ensure completion of a Port Facility Security Assessment for each of the port facilities, located within its territory, serving ships engaged on international voyages. The Contracting Government, a Designated Authority or a Recognized Security Organization may carry out this assessment. The completed Port Facility Security Assessment has to be approved by the Contracting Government or the Designated Authority concerned. This approval cannot be delegated. Port Facility Security Assessments should be periodically reviewed.

1.17 The Port Facility Security Assessment is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack. Security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.

The assessment must include the following components:

- the perceived threat to port installations and infrastructure must be determined;
- the potential vulnerabilities identified; and
- the consequences of incidents calculated.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk. The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan.

1.18 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to designate a Port Facility Security Officer. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.19 The Port Facility Security Plan should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the port facility can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may be issued by those responding at security level 3 to a security incident or threat thereof.

1.20 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to have, and operate in accordance with, a Port Facility Security Plan approved by the Contracting Government or by the Designated Authority concerned. The Port Facility Security Officer should implement its provisions and monitor the continuing effectiveness and relevance of the plan, including commissioning internal audits of the application of the plan. Amendments to any of the elements of an approved plan, for which the Contracting Government or the Designated Authority concerned has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation at the port facility. The Contracting Government or the Designated Authority concerned may test the effectiveness of the plan. The Port Facility Security Assessment covering the port facility or on which the development of the plan has been based should be regularly reviewed. All these activities may lead to amendment of the approved plan. Any amendments to specified elements of an approved plan will have to be submitted for approval by the Contracting Government or by the Designated Authority concerned.

1.21 Ships using port facilities may be subject to the port State control inspections and additional control measures outlined in regulation XI-2/9. The relevant authorities may request the provision of information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port. There may be circumstances in which entry into port could be denied.

Information and communication

1.22 Chapter XI-2 and part A of this Code require Contracting Governments to provide certain information to the International Maritime Organization and for information to be made available to allow effective communication between Contracting Governments and between Company/Ship Security Officers and the Port Facility Security Officers.

2 DEFINITIONS

2.1 No guidance is provided with respect to the definitions set out in chapter XI-2 or part A of this Code.

2.2 For the purpose of this Part of the Code:

- .1 “section” means a section of part A of the Code and is indicated as “section A/ <followed by the number of the section>”;
- .2 “paragraph” means a paragraph of this Part of the Code and is indicated as “paragraph <followed by the number of the paragraph>”; and
- .3 “Contracting Government”, when used in paragraphs 14 to 18, means the “Contracting Government within whose territory the port facility is located” and includes a reference to the “Designated Authority”.

3 APPLICATION

General

3.1 The guidance given in this Part of the Code should be taken into account when implementing the requirements of chapter XI-2 and part A of this Code.

3.2 However, it should be recognized that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship.

3.3 Similarly, in relation to the guidance on port facilities, the extent to which this guidance applies will depend on the port facilities, the types of ships using the port facility, the types of cargo and/or passengers and the trading patterns of visiting ships.

3.4 The provisions of chapter XI-2 and part A of this Code are not intended to apply to port facilities designed and used primarily for military purposes.

4 RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

Security of assessments and plans

4.1 Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans, and to individual assessments or plans.

Designated authorities

4.2 Contracting Governments may identify a Designated Authority within Government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of this Code.

Recognized Security Organizations

4.3 Contracting Governments may authorize a Recognized Security Organization (RSO) to undertake certain security related activities, including:

- .1 approval of Ship Security Plans, or amendments thereto, on behalf of the Administration;*
- .2 verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of this Code on behalf of the Administration;
and
- .3 conducting Port Facility Security Assessments required by the Contracting Government.

4.4 An RSO may also advise or provide assistance to Companies or port facilities on security matters, including Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans. This can include completion of a Ship Security Assessment or Plan or Port Facility Security Assessment or Plan. If an RSO has done so in respect of a ship security assessment or plan that RSO should not be authorized to approve that ship security plan.

4.5 When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

- .1 expertise in relevant aspects of security;**
- .2 appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;**
- .3 their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimise such risks;**
- .4 their ability to maintain and improve the expertise of their personnel;**
- .5 their ability to monitor the continuing trustworthiness of their personnel;**
- .6 their ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material;**
- .7 their knowledge of the requirements chapter XI-2 and part A of this Code and relevant national and international legislation and security requirements;**
- .8 their knowledge of current security threats and patterns;**
- .9 their knowledge on recognition and detection of weapons, dangerous substances and devices;**
- .10 their knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;**
- .11 their knowledge on techniques used to circumvent security measures; and**
- .12 their knowledge of security and surveillance equipment and systems and their operational limitations.**

When delegating specific duties to a RSO, Contracting Governments, including Administrations, should ensure that the RSO has the competencies needed to undertake the task.

4.6 A Recognized Organization, as defined in regulation I/6 and fulfilling the requirements of regulation XI-1/1, may be appointed as a RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

4.7 A Port or Harbour Authority or Port Facility operator may be appointed as a RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

Setting the security level

4.8 *In setting the security level Contracting Governments should take account of general and specific threat information. Contracting Governments should set the security level applying to ships or port facilities at one of three levels:*

- *Security level 1: normal, the level at which the ship or port facility normally operates;*
- Security level 2: heightened, the level applying for as long as there is a heightened risk of a security incident; and
- Security level 3: exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

4.9 Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

4.10 *At all times the Master of a ship has the ultimate responsibility for the safety and security of the ship. Even at security level 3 a Master may seek clarification or amendment of instructions issued by those responding to a security incident, or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.*

4.11 The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liaise at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility. Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility's security level and should provide the ship with any relevant security information.

4.12 While there may be circumstances when an individual ship may be operating at a higher security level than the port facility it is visiting, there will be no circumstances

when a ship can have a lower security level than the port facility it is visiting. If a ship has a higher security level than the port facility it intends to use, the CSO or SSO should advise the PFSO without delay. The PFSO should undertake an assessment of the particular situation in consultation with the CSO or SSO and agree on appropriate security measures with the ship, which may include completion and signing of a Declaration of Security.

4.13 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly. Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to ship and CSO and SSO. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish means of notifying PFSOs of changes in security levels. Contracting Governments should compile and maintain the contact details for a list of those who need to be informed of changes in security levels. Whereas the security level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the type and detail of the information conveyed and the method by which it is conveyed, to SSOs, CSOs and PFSOs.

Contact points and information on Port Facility Security Plans

4.14 Where a port facility has a PFSP, that fact has to be communicated to the Organization and that information must also be made available to Company and Ship Security Officers. No further details of the PFSP have to be published other than that it is in place. Contracting Governments should consider establishing either central or regional points of contact, or other means of providing up to date information on the locations where PFSPs are in place, together with contact details for the relevant PFSO. The existence of such contact points should be publicised. They could also provide information on the recognized security organizations appointed to act on behalf of the Contracting Government, together with details of the specific responsibility and conditions of authority delegated to such recognized security organizations.

4.15 In the case of a port that does not have a PFSP (and therefore does not have a PFSO) the central or regional point of contact should be able to identify a suitably qualified person ashore who can arrange for appropriate security measures to be in place, if needed, for the duration of the ship's visit.

4.16 Contracting Governments should also provide the contact details of Government officers to whom an SSO, a CSO and a PFSO can report security concerns. These Government officers should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting Government. In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate. For this purpose, the

contact details of the Government officers should be communicated to the International Maritime Organization.

4.17 Contracting Governments should also make the information indicated in paragraphs 4.14 to 4.16, available to other Contracting Governments on request.

Identification documents

4.18 *Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.*

Fixed and floating platforms and mobile offshore drilling units on location

4.19 *Contracting Governments should consider establishing appropriate security measures for fixed and floating platforms and mobile offshore drilling units on location to allow interaction with ships which are required to comply with the provisions of chapter XI-2 and part A of this Code¹⁸.*

Ships which are not required to comply with part A of this Code

4.20 Contracting Governments should consider establishing appropriate security measures to enhance the security of ships to which this chapter XI-2 and part A of this Code does not apply and to ensure that any security provisions applying to such ships allow interaction with ships to which part A of this Code applies.

Threats to ships and other incidents at sea

4.21 Contracting Governments should provide general guidance on the measures considered appropriate to reduce the security risk to ships flying their flag when at sea. They should provide specific advice on the action to be taken in accordance with security levels 1 to 3, if:

- .1 there is a change in the security level applying to the ship while it is at sea, e.g. because of the geographical area in which it is operating or relating to the ship itself; and

¹⁸ Refer to Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling units on location and fixed and floating platforms not covered by chapter XI-2 of 1974 SOLAS Convention, adopted by the Conference on Maritime Security by resolution 7.

- .2 there is a security incident or threat thereof involving the ship while at sea.

Contracting Governments should establish the best methods and procedures for these purposes. In the case of an imminent attack the ship should seek to establish direct communication with those responsible in the flag State for responding to security incidents.

4.22 Contracting Governments should also establish a point of contact for advice on security for any ship:

- .1 entitled to fly their flag; or
- .2 operating in their territorial sea or having communicated an intention to enter their territorial sea.

4.23 Contracting Governments should offer advice to ships operating in their territorial sea or having communicated an intention to enter their territorial sea, which could include advice:

- .1 to alter or delay their intended passage;
- .2 to navigate on a particular course or proceed to a specific location;
- .3 on the availability of any personnel or equipment that could be placed on the ship;

- .4 to co-ordinate the passage, arrival into port or departure from port, to allow escort by patrol craft or aircraft (fixed-wing or helicopter).

Contracting Governments should remind ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, of any temporary restricted areas that they have published.

4.24 Contracting Governments should recommend that ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, implement expeditiously, for the ship's protection and for the protection of other ships in the vicinity, any security measure the Contracting Government may have advised.

4.25 The plans prepared by the Contracting Governments for the purposes given in paragraph 4.22 should include information on an appropriate point of contact, available on a 24-hour basis, within the Contracting Government including the Administration. These plans should also include information on the circumstances in which the Administration considers assistance should be sought from nearby coastal States, and a procedure for liaison between port facility security officers and ship security officers.

Alternative security agreements

4.26 Contracting Governments, in considering how to implement chapter XI-2 and part A of this Code, may conclude one or more agreements with one or more Contracting Governments. The scope of an agreement is limited to short international voyages on

fixed routes between port facilities in the territory of the parties to the agreement. When concluding an agreement, and thereafter, the Contracting Governments should consult other Contracting Governments and Administrations with an interest in the effects of the agreement. Ships flying the flag of a State that is not party to the agreement should only be allowed to operate on the fixed routes covered by the agreement if their Administration agrees that the ship should comply with the provisions of the agreement and requires the ship to do so. In no case can such an agreement compromise the level of security of other ships and port facilities not covered by it, and specifically, all ships covered by such an agreement may not conduct ship-to-ship activities with ships not so covered. Any operational interface undertaken by ships covered by the agreement should be covered by it.

The operation of each agreement must be continually monitored and amended when the need arises and in any event should be reviewed every 5 years.

Equivalent arrangements for port facilities

4.27 For certain specific port facilities with limited or special operations but with more than occasional traffic, it may be appropriate to ensure compliance by security measures equivalent to those prescribed in chapter XI-2 and in part A of this Code. This can, in particular, be the case for terminals such as those attached to factories, or quaysides with no frequent operations.

Manning level

4.28 In establishing the minimum safe manning of a ship the Administration should take into account¹⁹ that the minimum safe manning provisions established by regulation V/14²⁰ only address the safe navigation of the ship. The Administration should also take into account any additional workload which may result from the implementation of the ship's security plan and ensure that the ship is sufficiently and effectively manned. In doing so the Administration should verify that ships are able to implement the hours of rest and other measures to address fatigue which have been promulgated by national law, in the context of all shipboard duties assigned to the various shipboard personnel.

¹⁹ Refer to Further Work by the International Maritime Organization pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution 3, inviting, amongst others, the Organization to review Assembly Resolution A.890(21) on Principles of Safe Manning. This review may also lead to amendments of regulation V/14.

²⁰ As was in force on the date of adoption of this Code.

Control and compliance measures²¹

General

4.29 *Regulation XI-2/9 describes the control and compliance measures applicable to ships under chapter XI-2. It is divided into three distinct sections; control of ships already in a port, control of ships intending to enter a port of another Contracting Government, and additional provisions applicable to both situations.*

4.30 *Regulation XI-2/9.1, control of ships in port, implements a system for the control of ships while in the port of a foreign country where duly authorized officers of the Contracting Government (duly authorized officers) have the right to go on board the ship to verify that the required certificates are in proper order. Then if there are clear grounds to believe the ship does not comply, control measures such as additional inspections or detention may be taken. This reflects current control systems²². Regulation XI-2/9.1 builds on such systems and allows for additional measures (including expulsion of a ship from a port to be taken as a control measure) when duly authorized officers have clear grounds for believing that a ship is in non-compliance with the requirements of chapter XI-2 or part A of this Code. Regulation XI-2/9.3 describes the safeguards that promote fair and proportionate implementation of these additional measures.*

²¹ Refer to Further Work by the International Maritime Organization pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution 3, inviting, amongst others, the Organization to review Assembly Resolutions A.787(19) and A.882(21) on Procedures for Port State Control.

²² See regulation I/19 and regulation IX/6.2 of SOLAS 74 as amended, article 21 of LOADLINE 66 as modified by the 1988 LOADLINE Protocol, articles 5 and 6, regulation 8A of Annex I, regulation 15 of Annex II of MARPOL 73/78 as amended, article X of STCW 78 as amended and IMO Assembly Resolutions A.787(19) and A.882(21).

4.31 Regulation XI-2/9.2 applies control measures to ensure compliance to ships intending to enter a port of another Contracting Government and introduces an entirely different concept of control within chapter XI-2, applying to security only. Under this regulation measures may be implemented prior to the ship entering port, to better ensure security. Just as in regulation XI-2/9.1, this additional control system is based on the concept of clear grounds for believing the ship does not comply with chapter XI-2 or part A of this Code, and includes significant safeguards in regulations XI-2/9.2.2 and XI-2/9.2.5 as well as in regulation XI-2/9.3.

4.32 Clear grounds that the ship is not in compliance means evidence or reliable information that the ship does not correspond with the requirements of chapter XI-2 or part A of this Code, taking into account the guidance given in this Part of the Code. Such evidence or reliable information may arise from the duly authorized officer's professional judgement or observations gained while verifying the ship's International Ship Security Certificate or Interim International Ship Security Certificate issued in accordance with part A of this Code (certificate) or from other sources. Even if a valid certificate is on board the ship, the duly authorized officers may still have clear grounds for believing that the ship is not in compliance based on their professional judgment.

4.33 Examples of possible clear grounds under regulations XI-2/9.1 and XI-2/9.2 may include, when relevant:

- .1 evidence from a review of the certificate that it is not valid or it has expired;*
- .2 evidence or reliable information that serious deficiencies exist in the security equipment, documentation or arrangements required by chapter XI-2 and part A of this Code;*
- .3 receipt of a report or complaint which, in the professional judgment of the duly authorized officer, contains reliable information clearly indicating that the ship does not comply with the requirements of chapter XI-2 or part A of this Code;*

- .4 evidence or observation gained by a duly authorized officer using professional judgment that the master or ship's personnel is not familiar with essential shipboard security procedures or cannot carry out drills related to the security of the ship or that such procedures or drills have not been carried out;**
- .5 evidence or observation gained by a duly authorized officer using professional judgment that key members ship's personnel are not able to establish proper communication with any other key members of ship's personnel with security responsibilities on board the ship;**
- .6 evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another ship where either the port facility or the other ship is in violation of chapter XI-2 or part A of this Code, and the ship in question has not completed a Declaration of Security, nor taken appropriate, special or additional security measures or has not maintained appropriate ship security procedures;**
- .7 evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another source (e.g., another ship or helicopter transfer) where either the port facility or the other source is not required to comply with chapter XI-2 or part A of this Code, and the ship has not taken appropriate, special or additional security measures or has not maintained appropriate security procedures; and**
- .8 if the ship holds a subsequent, consecutively issued Interim International Ship Security Certificate as described in section A/19.4, and if, in the professional judgment of an officer duly authorized, one of the purposes of the ship or a Company in requesting such a certificate is to avoid full compliance with chapter XI-2 and part A of this Code beyond the period of the initial interim certificate as described in section A/19.4.4.**

4.34 The international law implications of regulation XI-2/9 are particularly relevant, and the regulation should be implemented with regulation XI-2/2.4 in mind, as the potential exists for situations where either measures will be taken which fall outside the scope of chapter XI-2, or where rights of affected ships, outside chapter XI-2, should be considered. Thus, regulation XI-2/9 does not prejudice the Contracting Government from taking measures having a basis in, and consistent with, international law, to ensure the safety or security of persons, ships, port facilities and other property in cases where the ship, although in compliance with chapter XI-2 and part A of this Code, is still considered to present a security risk.

4.35 When a Contracting Government imposes control measures on a ship, the Administration should, without delay, be contacted with sufficient information to enable the Administration to fully liaise with the Contracting Government.

Control of ships in port

4.36 Where the non-compliance is either a defective item of equipment or faulty documentation leading to the ship's detention and the non-compliance cannot be remedied in the port of inspection, the Contracting Government may allow the ship to sail to another port provided that any conditions agreed between the port States and the Administration or master are met.

Ships intending to enter the port of another Contracting Government

4.37 Regulation XI-2/9.2.1 lists the information Contracting Governments may require from a ship as a condition of entry into port. One item of information listed is confirmation of any special or additional measures taken by the ship during its last ten calls at a port facility. Examples could include:

- .1 records of the measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments; and*
- .2 any Declarations of Security that were entered into with port facilities or other ships.*

4.38 *Another item of information listed, that may be required as a condition of entry into port, is confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility. It would not normally be required to include records of transfers of pilots, customs, immigration, security officials nor bunkering, lightering, loading of supplies and unloading of waste by ship within port facilities as these would normally fall within the auspices of the Port Facility Security Plan. Examples of information that might be given include:*

- .1 records of the measures taken while engaged in a ship to ship activity with a ship flying the flag of a State which is not a Contracting Government especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;**
- .2 records of the measures taken while engaged in a ship to ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions of chapter XI-2 and part A of this Code such as a copy of any security certificate issued to that ship under other provisions; and**
- .3 in the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of this Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of this Code to provide States with enough appropriate information to maintain their security integrity.**

4.39 *Examples of other practical security related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:*

- .1 information contained in the Continuous Synopsis Record;**

- .2 location of the ship at the time the report is made;**
- .3 expected time of arrival of the ship in port;**
- .4 crew list;**
- .5 general description of cargo aboard the ship;**
- .6 passenger list; and**
- .7 information required to be carried under regulation XI-2/5.**

4.40 *Regulation XI-2/9.2.5 allows the master of a ship, upon being informed that the coastal or port State will implement control measures under regulation XI-2/9.2, to withdraw the intention for the ship to enter port. If the master withdraws that intention, regulation XI-2/9 no longer applies, and any other steps that are taken must be based on, and consistent with, international law.*

Additional provisions

4.41 *In all cases where a ship is denied entry or expelled from a port, all known facts should be communicated to the authorities of relevant States. This communication should consist of the following when known:*

- .1 name of ship, its flag, the ship's identification number, call sign, ship type and cargo;**

- .2 reason for denying entry or expulsion from port or port areas;**
- .3 if relevant, the nature of any security non-compliance;**
- .4 if relevant, details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage;**
- .5 past port(s) of call and next declared port of call;**
- .6 time of departure and likely estimated time of arrival at those ports;**
- .7 any instructions given to ship, e.g., reporting on route;**
- .8 available information on the security level at which the ship is currently operating;**
- .9 information regarding any communications the port State has had with the Administration;**
- .10 contact point within the port State making the report for the purpose of obtaining further information;**
- .11 crew list; and**
- .12 any other relevant information.**

4.42 *Relevant States to contact should include those along the ship's intended passage to its next port, particularly if the ship intends to enter the territorial sea of that coastal State. Other relevant States could include previous ports of call, so that further information might be obtained and security issues relating to the previous ports resolved.*

4.43 *In exercising control and compliance measures, the duly authorized officers should ensure that any measures or steps imposed are proportionate. Such measures or steps should be reasonable and of the minimum severity and duration necessary to rectify or mitigate the non-compliance.*

4.44 *The word "delay" in regulation XI-2/9.3.5.1 also refers to situations where, pursuant to actions taken under this regulation, the ship is unduly denied entry into port or the ship is unduly expelled from port.*

Non-party ships and ships below convention size

4.45 With respect to ships flying the flag of a State which is not a Contracting Government to the Convention and not a Party to the 1988 SOLAS Protocol²³, Contracting Governments should not give more favourable treatment to such ships. Accordingly, the requirements of regulation XI-2/9 and the guidance provided in this Part of the Code should be applied to those ships.

4.46 Ships below Convention size are subject to measures by which States maintain security. Such measures should be taken with due regard to the requirements in chapter XI-2 and the guidance provided in this Part of the Code.

5 **DECLARATION OF SECURITY**

General

²³ Protocol of 1988 relating to the International Convention for the Safety of Life at Sea, 1974.

5.1 *A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary or when a ship deems it necessary.*

5.1.1 *The need for a DoS may be indicated by the results of the Port Facility Security Assessment (PFSA) and the reasons and circumstances in which a DoS is required should be set out in the Port Facility Security Plan (PFSP).*

5.1.2 The need for a DoS may be indicated by an Administration for ships entitled to fly its flag or as a result of a ship security assessment and should be set out in the ship security plan.

5.2 *It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, or another ship with which it interfaces, and for ship/port interface or ship to ship activities that pose a higher risk to persons, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors.*

5.2.1 In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the Port Facility Security Officer (PFSO) or Ship Security Officer (SSO) should acknowledge the request and discuss appropriate security measures.

5.3 *A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous goods or hazardous substances. The PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.*

5.4 The main purpose of a DoS is to ensure agreement is reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans.

5.4.1 The agreed DoS should be signed and dated by both the port facility and the ship(s), as applicable, to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level, or levels and the relevant contact details.

5.4.2 A change in the security level may require that a new or revised DoS be completed.

5.5 The DoS should be completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships, as applicable.

5.6 A model DoS is included in Appendix 1 to this Part of the Code. This model is for a DoS between a ship and a port facility. If the DoS is to cover two ships this model should be appropriately adjusted.

General

6.1 Regulation XI-2/5 requires the company to provide the master of the ship with information to meet the requirements of the Company under the provisions of this regulation. This information should include items such as:

- .1 parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries (for example, retail sales outlets, casinos, etc.);
- .2 parties responsible for deciding the employment of the ship including, time or bareboat charterer(s) or any other entity acting in such capacity; and
- .3 in cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers.

6.2 In accordance with regulation XI-2/5 the Company is obliged to update and keep this information current as and when changes occur.

6.3 This information should be in English, French or Spanish language.

6.4 With respect to ships constructed before 1 July 2004, this information should reflect the actual condition on that date.

6.5 With respect to ships constructed on or after 1 July 2004 and for ships constructed before 1 July 2004 which were out of service on 1 July 2004, the information should be provided as from the date of entry of the ship into service and should reflect the actual condition on that date.

6.6 After 1 July 2004 when a ship is withdrawn from service the information should be provided as from the date of re-entry of the ship into service and should reflect the actual condition on that date.

6.7 Previously provided information that does not relate to the actual condition on that date need not be retained on board.

6.8 When the responsibility for the operation of the ship is assumed by another Company, the information relating to the Company, which operated the ship, is not required to be left on board.

In addition other relevant guidance is provided under sections 8, 9 and 13.

7 SHIP SECURITY

Relevant guidance is provided under sections 8, 9 and 13.

8 SHIP SECURITY ASSESSMENT

Security assessment

8.1 *The Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each of the ships in the Company's fleet which is required to comply with the provisions of chapter XI-2 and part A of this Code for which the CSO is responsible. While the CSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.*

8.2 *Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs. Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment. The CSO should follow any specific guidance offered by the Contracting Governments.*

8.3 *A SSA should address the following elements on board or within the ship:*

- .1 physical security;**
- .2 structural integrity;**
- .3 personnel protection systems;**
- .4 procedural policies;**
- .5 radio and telecommunication systems, including computer systems and networks; and**
- .6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.**

8.4 *Those involved in a SSA should be able to draw upon expert assistance in relation to:*

- .1 knowledge of current security threats and patterns;**
- .2 recognition and detection of weapons, dangerous substances and devices;**
- .3 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;**
- .4 techniques used to circumvent security measures;**
- .5 methods used to cause a security incident;**
- .6 effects of explosives on ship's structures and equipment;**
- .7 ship security;**
- .8 ship/port interface business practices;**
- .9 contingency planning, emergency preparedness and response;**
- .10 physical security;**
- .11 radio and telecommunications systems, including computer systems and networks;**
- .12 marine engineering; and**
- .13 ship and port operations.**

8.5 *The CSO should obtain and record the information required to conduct an assessment, including:*

- .1 the general layout of the ship;**
- .2 the location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.;**
- .3 the location and function of each actual or potential access point to the ship;**
- .4 changes in the tide which may have an impact on the vulnerability or security of the ship;**
- .5 the cargo spaces and stowage arrangements;**
- .6 the locations where the ship's stores and essential maintenance equipment is stored;**
- .7 the locations where unaccompanied baggage is stored;**
- .8 the emergency and stand-by equipment available to maintain essential services;**
- .9 the number of ship's personnel, any existing security duties and any existing training requirement practises of the Company;**
- .10 existing security and safety equipment for the protection of passengers and ship's personnel;**
- .11 escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;**
- .12 existing agreements with private security companies providing ship/waterside security services; and**
- .13 existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.**

8.6 The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to

breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

8.7 The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:

- .1 the restricted areas;**
- .2 the response procedures to fire or other emergency conditions;**
- .3 the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;**
- .4 the frequency and effectiveness of security patrols;**
- .5 the access control systems, including identification systems;**
- .6 the security communications systems and procedures;**
- .7 the security doors, barriers and lighting; and**
- .8 the security and surveillance equipment and systems, if any.**

8.8 The SSA should consider the persons, activities, services and operations that it is important to protect. This includes:

- .1 the ship's personnel;**
- .2 passengers, visitors, vendors, repair technicians, port facility personnel, etc;**
- .3 the capacity to maintain safe navigation and emergency response;**
- .4 the cargo, particularly dangerous goods or hazardous substances;**
- .5 the ship's stores;**
- .6 the ship security communication equipment and systems, if any; and**
- .7 the ship's security surveillance equipment and systems, if any.**

8.9 The SSA should consider all possible threats, which may include the following types of security incidents:

- .1 damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;**
- .2 hijacking or seizure of the ship or of persons on board;**
- .3 tampering with cargo, essential ship equipment or systems or ship's stores;**
- .4 unauthorized access or use, including presence of stowaways;**
- .5 smuggling weapons or equipment, including weapons of mass destruction;**
- .6 use of the ship to carry those intending to cause a security incident and/or their equipment;**
- .7 use of the ship itself as a weapon or as a means to cause damage or destruction;**
- .8 attacks from seaward whilst at berth or at anchor; and**
- .9 attacks whilst at sea.**

8.10 *The SSA should take into account all possible vulnerabilities, which may include:*

- .1 conflicts between safety and security measures;**
- .2 conflicts between shipboard duties and security assignments;**
- .3 watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;**
- .4 any identified security training deficiencies; and**
- .5 any security equipment and systems, including communication systems.**

8.11 The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the

convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

8.12 Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

8.13 If the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO.

On-scene security survey

8.14 *The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:*

- .1 ensuring the performance of all ship security duties;**
- .2 monitoring restricted areas to ensure that only authorized persons have access;**
- .3 controlling access to the ship, including any identification systems;**
- .4 monitoring of deck areas and areas surrounding the ship;**
- .5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);**
- .6 supervising the handling of cargo and the delivery of ship's stores; and**
- .7 ensuring that ship security communication, information, and equipment are readily available.**

9 SHIP SECURITY PLAN

General

9.1 *The Company Security Officer (CSO) has the responsibility of ensuring that a Ship Security Plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security*

Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

9.2 All SSPs should:

- .1 detail the organizational structure of security for the ship;**
- .2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;**
- .3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;**
- .4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;**
- .5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;**
- .6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and**
- .7 reporting procedures to the appropriate Contracting Governments contact points.**

9.3 Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

9.4 *All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognized Security Organization (RSO) to review or approve the SSP the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.*

9.5 *CSOs and Ship Security Officers (SSOs) should develop procedures to:*

- .1 assess the continuing effectiveness of the SSP; and*
- .2 prepare amendments of the plan subsequent to its approval.*

9.6 *The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and part A of this Code will be carried out. Otherwise the process of issue to the ship of the required International Ship Security Certificate cannot be carried out. If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by, the Administration.*

Organization and performance of ship security duties

9.7 *In addition to the guidance given in section 9.2, the SSP should establish the following which relate to all security levels:*

- .1 the duties and responsibilities of all shipboard personnel with a security role;**
- .2 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;**
- .3 the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;**
- .4 the procedures and practices to protect security sensitive information held in paper or electronic format;**

- .5 the type and maintenance requirements, of security and surveillance equipment and systems, if any;**
- .6 the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and**
- .7 procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.**

9.8 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:

- .1 access to the ship by ship's personnel, passengers, visitors, etc;**
- .2 restricted areas on the ship;**
- .3 handling of cargo;**
- .4 delivery of ship's stores;**
- .5 handling unaccompanied baggage; and**
- .6 monitoring the security of the ship.**

Access to the ship

9.9 *The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:*

- .1 access ladders;**
- .2 access gangways;**
- .3 access ramps;**
- .4 access doors, side scuttles, windows and ports;**
- .5 mooring lines and anchor chains; and**
- .6 cranes and hoisting gear.**

9.10 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

9.11 The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship's personnel and visitors respectively. Any ship identification system should, when it is practicable to do so, be co-ordinated with that applying to the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

9.12 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and to the national or local authorities with security responsibilities.

9.13 The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

9.14 At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

- .1 checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc;*
- .2 in liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry on items), personal effects, vehicles and their contents can take place;*
- .3 in liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger*

ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;

- .4 segregating checked persons and their personal effects from unchecked persons and their personal effects;
- .5 segregating embarking from disembarking passengers;
- .6 **identification of access points that should be secured or attended to prevent unauthorized access;**
- .7 **securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and**
- .8 **providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.**

9.15 At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

9.16 At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

- .1 assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;**
- .2 limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;**
- .3 deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;**
- .4 establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;**
- .5 increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;**
- .6 escorting visitors on the ship;
- .7 providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and
- .8 carrying out a full or partial search of the ship.

Security Level 3

9.17 *At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:*

- .1 limiting access to a single, controlled, access point;**
- .2 granting access only to those responding to the security incident or threat thereof;
- .3 directions of persons on board;
- .4 suspension of embarkation or disembarkation;**
- .5 suspension of cargo handling operations, deliveries etc;
- .6 evacuation of the ship;**
- .7 movement of the ship; and
- .8 preparing for a full or partial search of the ship.

Restricted areas on the ship

9.18 *The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:*

- .1** prevent unauthorized access;
- .2** protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;
- .3** protect sensitive security areas within the ship; and
- .4** protect cargo and ship's stores from tampering.

9.19 *The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas them.*

9.20 *The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.*

9.21 *Restricted areas may include:*

- .1** navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;
- .2** spaces containing security and surveillance equipment and systems and their controls and lighting system controls;
- .3** ventilation and air-conditioning systems and other similar spaces;
- .4** spaces with access to potable water tanks, pumps, or manifolds;
- .5** spaces containing dangerous goods or hazardous substances;

- .6 spaces containing cargo pumps and their controls;**
- .7 cargo spaces and spaces containing ship's stores;**
- .8 crew accommodation; and**
- .9 any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.**

Security Level 1

9.22 *At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:*

- .1 locking or securing access points;**
- .2 using surveillance equipment to monitor the areas;**
- .3 using guards or patrols; and**
- .4 using automatic intrusion detection devices to alert the ship's personnel of unauthorized access.**

Security Level 2

9.23 *At security level 2, the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorized persons have access. The SSP should establish the additional security measures to be applied, which may include:*

- .1 establishing restricted areas adjacent to access points;**
- .2 continuously monitoring surveillance equipment; and**
- .3 dedicating additional personnel to guard and patrol restricted areas.**

Security Level 3

9.24 *At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:*

- .1 setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and
- .2 searching of restricted areas as part of a search of the ship.

Handling of cargo

9.25 *The security measures relating to cargo handling should:*

- .1 prevent tampering; and
- .2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

9.26 *The security measures, some of which may have to be applied in liaison with the port facility, should include inventory control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.*

Security Level 1

9.27 *At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:*

- .1 routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations;
- .2 checks to ensure that cargo being loaded matches the cargo documentation;
- .3 ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and
- .4 checking of seals or other methods used to prevent tampering.

9.28 *Checking of cargo may be accomplished by the following means:*

- .1** visual and physical examination; and
- .2** using scanning/detection equipment, mechanical devices, or dogs.

9.29 When there are regular, or repeated, cargo movement the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

Security Level 2

9.30 *At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:*

- .1** detailed checking of cargo, cargo transport units and cargo spaces;
- .2** intensified checks to ensure that only the intended cargo is loaded;
- .3** intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships; and
- .4** increased frequency and detail in checking of seals or other methods used to prevent tampering.

9.31 *Detailed checking of cargo may be accomplished by the following means:*

- .1** increasing the frequency and detail of visual and physical examination;
- .2** increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and
- .3** co-ordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

Security Level 3

9.32 *At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:*

- .1** suspension of the loading or unloading of cargo; and
- .2** verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Delivery of ship's stores

9.33 The security measures relating to the delivery of ship's stores should:

- .1** ensure checking of ship's stores and package integrity;
- .2** prevent ship's stores from being accepted without inspection;
- .3** prevent tampering; and
- .4** prevent ship's stores from being accepted unless ordered.

9.34 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

9.35 **At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:**

- .1** checking to ensure stores match the order prior to being loaded on board;
and
- .2** ensuring immediate secure stowage of ship's stores.

Security Level 2

9.36 At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

Security Level 3

9.37 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 subjecting ship's stores to more extensive checking;
- .2 preparation for restriction or suspension of handling of ship's stores; and
- .3 refusal to accept ship's stores on board the ship.

Handling unaccompanied baggage

9.38 The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship. It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

9.39 At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

9.40 At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

9.41 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
- .2 preparation for restriction or suspension of handling of unaccompanied baggage; and
- .3 refusal to accept unaccompanied baggage on board the ship.

Monitoring the Security of the Ship

9.42 *The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:*

- .1 *lighting;***
- .2 *watch-keepers, security guards and deck watches including patrols; and***
- .3 *automatic intrusion detection devices and surveillance equipment.***

9.43 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

9.44 The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

Security Level 1

9.45 *At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.*

9.46 *The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary. While underway, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulations for the Prevention of Collisions at Sea in force. The following should be considered when establishing the appropriate level and location of lighting:*

- .1** the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;
- .2** coverage should include the area on and around the ship;
- .3** coverage should facilitate personnel identification at access points; and
- .4** coverage may be provided through coordination with the port facility.

Security Level 2

9.47 *At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:*

- .1** increasing the frequency and detail of security patrols;
- .2** increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;
- .3** assigning additional personnel as security lookouts; and
- .4** ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided.

9.48 *Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.*

Security Level 3

9.49 *At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:*

- .1** switching on of all lighting on, or illuminating the vicinity of, the ship;
- .2** switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;
- .3** maximising the length of time such surveillance equipment can continue to record;
- .4** preparation for underwater inspection of the hull of the ship; and
- .5** initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

Differing security levels

9.50 *The SSP should establish details of the procedures and security measures the ship could adopt if the ship is at a higher security level than that applying to a port facility.*

Activities not covered by the Code

9.51 *The SSP should establish details of the procedures and security measures the ship should apply when:*

- .1 it is at a port of a State which is not a Contracting Government;*
- .2 it is interfacing with a ship to which this Code does not apply²⁴;*
- .3 it is interfacing with fixed or floating platforms or a mobile drilling unit on location; or*
- .4 it is interfacing with a port or port facility which is not required to comply with chapter XI-2 and part A of this Code.*

Declarations of security

9.52 *The SSP should detail how requests for DoS from a port facility will be handled and the circumstances under which the ship itself should request a DoS.*

Audit and review

9.53 *The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.*

10 RECORDS

General

10.1 Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of ship security plans are being implemented.

²⁴ Refer to further work by the International Maritime Organization pertaining to Enhancement of maritime security and to Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling units on location and fixed and floating platforms not covered by chapter XI-2 of the 1974 SOLAS Convention, adopted by the Conference on Maritime Security by resolutions 3 and 7 respectively.

10.2 Records may be kept in any format but should be protect from unauthorized access or disclosure.

11 COMPANY SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

12 SHIP SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

Training

13.1 The Company Security Officer (CSO) and appropriate shore based Company personnel, and the Ship Security Officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

- .1 security administration;**
- .2 relevant international conventions, codes and recommendations;**
- .3 relevant Government legislation and regulations;**

- .4 responsibilities and functions of other security organizations;**
- .5 methodology of ship security assessment;**
- .6 methods of ship security surveys and inspections;**
- .7 ship and port operations and conditions;**
- .8 ship and port facility security measures;**
- .9 emergency preparedness and response and contingency planning;**
- .10 instruction techniques for security training and education, including security measures and procedures;**
- .11 handling sensitive security related information and security related communications;
- .12 knowledge of current security threats and patterns;
- .13 recognition and detection of weapons, dangerous substances and devices;
- .14 recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;**
- .15 techniques used to circumvent security measures;
- .16 security equipment and systems and their operational limitations;
- .17 methods of conducting audits, inspection, control and monitoring;**
- .18 methods of physical searches and non-intrusive inspections;**
- .19 security drills and exercises, including drills and exercises with port facilities; and
- .20 assessment of security drills and exercises.**

13.2 *In addition the SSO should have adequate knowledge of, and receive training, in some or all of the following, as appropriate:*

- .1 the layout of the ship;**
- .2 the ship security plan and related procedures (including scenario-based training on how to respond);**
- .3 crowd management and control techniques;

- .4 operations of security equipment and systems; and
- .5 testing, calibration and whilst at sea maintenance of security equipment and systems.

13.3 Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

- .1 knowledge of current security threats and patterns;
- .2 recognition and detection of weapons, dangerous substances and devices;
- .3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;**
- .4 techniques used to circumvent security measures;
- .5 crowd management and control techniques;
- .6 security related communications;
- .7 knowledge of the emergency procedures and contingency plans;
- .8 operations of security equipment and systems;
- .9 testing, calibration and whilst at sea maintenance of security equipment and systems;
- .10 inspection, control, and monitoring techniques; and**
- .11 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.**

13.4 All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:

- .1 the meaning and the consequential requirements of the different security levels;
- .2 knowledge of the emergency procedures and contingency plans;
- .3 recognition and detection of weapons, dangerous substances and devices;
- .4 recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and**
- .5 techniques used to circumvent security measures.

Drills and exercises

13.5 *The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security related deficiencies, which need to be addressed.*

13.6 To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship, within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as those security threats listed in paragraph 8.9.

13.7 Various types of exercises which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability, and response. These exercises may be:

- .1 full scale or live;
- .2 tabletop simulation or seminar; or
- .3 combined with other exercises held such as search and rescue or emergency response exercises.

13.8 Company participation in an exercise with another Contracting Government should be recognized by the Administration.

14 PORT FACILITY SECURITY
Relevant guidance is provided under section 15, 16 and 18.

15 PORT FACILITY SECURITY ASSESSMENT

General

15.1 The Port Facility Security Assessment (PFSA) may be conducted by a Recognized Security Organization (RSO). However, approval of a completed PFSA should only be given by the relevant Contracting Government.

15.2 *If a Contracting Government uses a RSO, to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.*

15.3 *A PFSA should address the following elements within a port facility:*

- .1** physical security;
- .2** structural integrity;
- .3** personnel protection systems;
- .4** procedural policies;
- .5** radio and telecommunication systems, including computer systems and networks;
- .6** relevant transportation infrastructure;
- .7** utilities; and
- .8** other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility.

15.4 *Those involved in a PFSA should be able to draw upon expert assistance in relation to:*

- .1** knowledge of current security threats and patterns;
- .2** recognition and detection of weapons, dangerous substances and devices;
- .3** recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- .4** techniques used to circumvent security measures;

- .5 methods used to cause a security incident;
- .6 effects of explosives on structures and port facility services;
- .7 port facility security;
- .8 port business practices;
- .9 contingency planning, emergency preparedness and response;
- .10 physical security measures e.g. fences;
- .11 radio and telecommunications systems, including computer systems and networks;
- .12 transport and civil engineering; and
- .13 ship and port operations.

Identification and evaluation of important assets and infrastructure it is important to protect

15.5 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established. This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident. This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

15.6 Identification and evaluation of assets and infrastructure should be used to prioritise their relative importance for protection. The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid re-establishment of normal functioning is possible.

15.7 Assets and infrastructure that should be considered important to protect may include:

- .1 accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;

- .2 cargo facilities, terminals, storage areas, and cargo handling equipment;
- .3 systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
- .4 port vessel traffic management systems and aids to navigation;
- .5 power plants, cargo transfer piping, and water supplies;
- .6 bridges, railways, roads;
- .7 port service vessels, including pilot boats, tugs, lighters etc;
- .8 security and surveillance equipment and systems; and
- .9 the waters adjacent to the port facility.

15.8 *The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritisation of protective measures, and decisions concerning the allocation of resources to better protect the port facility. The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.*

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures

15.9 *Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security requirements to enable planning and resource allocations. Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies. By identifying and assessing threats, those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.*

15.10 *The PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:*

- .1 any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack;

- .2 the likely consequences in terms of loss of life, damage to property, economic disruption, including disruption to transport systems, of an attack on, or at, the port facility;
- .3 the capability and intent of those likely to mount such an attack; and
- .4 the possible type, or types, of attack,

producing an overall assessment of the level of risk against which security measures have to be developed.

15.11 The PFSA should consider all possible threats, which may include the following types of security incidents:

- .1 damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism;**
- .2 hijacking or seizure of the ship or of persons on board;**
- .3 tampering with cargo, essential ship equipment or systems or ship's stores;**
- .4 unauthorized access or use including presence of stowaways;**
- .5 smuggling weapons or equipment, including weapons of mass destruction;**
- .6 use of the ship to carry those intending to cause a security incident and their equipment;
- .7 use of the ship itself as a weapon or as a means to cause damage or destruction;
- .8 blockage; of port entrances, locks, approaches etc; and**
- .9 nuclear, biological and chemical attack.**

15.12 The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification, selection, and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability

15.13 The identification and prioritisation of countermeasures is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship/port interface to the possible threats.

15.14 Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

- .1 security surveys, inspections and audits;*
- .2 consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;*
- .3 historical information on security incidents; and*
- .4 operations within the port facility.*

Identification of vulnerabilities

15.15 Identification of vulnerabilities in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges etc that could be resolved through physical measures, e.g. permanent barriers, alarms, surveillance equipment etc.

15.16 Identification of vulnerabilities should include consideration of:

- .1 waterside and shore-side access to the port facility and ships berthing at the facility;
- .2 structural integrity of the piers, facilities, and associated structures;
- .3 existing security measures and procedures, including identification systems;
- .4 existing security measures and procedures relating to port services and utilities;
- .5 measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;
- .6 adjacent areas that may be exploited during, or for, an attack;
- .7 existing agreements with private security companies providing waterside/shore-side security services;
- .8 any conflicting policies between safety and security measures and procedures;
- .9 any conflicting port facility and security duty assignments;
- .10 any enforcement and personnel constraints;
- .11 any deficiencies identified during training and drills; and
- .12 any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

16 PORT FACILITY SECURITY PLAN

General

16.1 *Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the Port Facility Security Officer (PFSO). While the PFSO need not necessarily personally undertake all the duties associated with the post the ultimate responsibility for ensuring that they are properly performed remains with the individual PFSO.*

16.2 *The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers. The Port Facility Security (PFSA) will have identified the particular features of the port facility, and of the potential security risks, that have led to the need to appoint a PFSO and to prepare a*

PFSP. The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in the PFSP and for appropriate security measures to be established so as to minimise the likelihood of a breach of security and the consequences of potential risks. Contracting Governments may prepare advice on the preparation and content of a PFSP.

16.3 All PFSPs should:

- .1 detail the security organization of the port facility,**
- .2 the organization's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organization and its links with others, including ships in port;**
- .3 detail the basic security level 1 measures, both operational and physical, that will be in place;**
- .4 detail the additional security measures that will allow the port facility to progress without delay to security level 2 and, when necessary, to security level 3;**
- .5 provide for regular review, or audit, of the PFSP and for its amendments in response to experience or changing circumstances; and**
- .6 reporting procedures to the appropriate Contracting Governments contact points.**

16.4 *Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.*

16.5 *Contracting Government should approve the PFSPs of the port facilities under their jurisdiction. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.*

16.6 *The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each*

measure will be in place. If there is likely to be any delay in their provision this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

16.7 The use of firearms on or near ships and in port facilities may pose particular and significant safety risks, in particular in connection with certain dangerous or hazardous substances and should be considered very carefully. In the event that a Contracting Government decides that it is necessary to use armed personnel in these areas, that Contracting Government should ensure that these personnel are duly authorized and trained in the use of their weapons and that they are aware of the specific risks to safety that are present in these areas. If a Contracting Government authorizes the use of firearms they should issue specific safety guidelines on their use. The PFSP should contain specific guidance on this matter in particular with regard its application to ships carrying dangerous goods or hazardous substances.

Organization and performance of port facility security duties

16.8 *In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:*

- .1 the role and structure of the port facility security organization;**
- .2 the duties, responsibilities and training requirements of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;**
- .3 the port facility security organization's links with other national or local authorities with security responsibilities;**
- .4 the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;**
- .5 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;**
- .6 the procedures and practices to protect security sensitive information held in paper or electronic format;**

- .7 the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;**
- .8 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;**
- .9 procedures relating to cargo handling;**
- .10 procedures covering the delivery of ship's stores;**
- .11 the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility;**
- .12 the means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches;**
- .13 the procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested; and**
- .14 the procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organizations.**

16.9 *The remainder of this section addresses specifically the security measures that could be taken at each security level covering:*

- .1 access to the port facility;**
- .2 restricted areas within the port facility;**
- .3 handling of cargo;**
- .4 delivery of ship's stores;**
- .5 handling unaccompanied baggage; and**
- .6 monitoring the security of the port facility.**

Access to the port facility

16.10 *The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA.*

16.11 For each of these the PFSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the PFSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

16.12 The PFSP should establish for each security level the means of identification required to allow access to the port facility and for individuals to remain within the port facility without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for port facility personnel and for visitors respectively. Any port facility identification system should, when it is practicable to do so, be co-ordinated with that applying to ships that regularly use the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The PFSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

16.13 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the port facility and their attempt to obtain access should be reported to the PFSO and to the national or local authorities with security responsibilities.

16.14 The PFSP should identify the locations where persons, personal effects, and vehicle searches are to be undertaken. Such locations should be covered to facilitate continuous operation regardless of prevailing weather conditions, in accordance with the frequency laid down in the PFSP. Once subjected to search persons, personal effects and vehicles should proceed directly to the restricted holding, embarkation or car loading areas.

16.15 The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking passengers, ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons.

16.16 The PFSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

16.17 At security level 1, the PFSP should establish the control points where the following security measures may be applied:

- .1 restricted areas which should be bound by fencing or other barriers to a standard which should be approved by the Contracting Government;
- .2 checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc;
- .3 checking vehicles used by those seeking entry to the port facility in connection with a ship;
- .4 **verification of the identity of port facility personnel and those employed within the port facility and their vehicles;**
- .5 **restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity;**
- .6 **undertaking searches of persons, personal effects, vehicles and their contents; and**
- .7 **identification of any access points not in regular use which should be permanently closed and locked.**

16.18 At security level 1, all those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the approved PFSP and should be specifically approved by the Contracting Government. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

16.19 At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

- .1 assigning additional personnel to guard access points and patrol perimeter barriers;**
- .2 limiting the number of access points to the port facility, and identify those to be closed and the means of adequately securing them;**
- .3 providing for means of impeding movement through the remaining access points, e.g. security barriers;**
- .4 increasing the frequency of searches of persons, personal effects, and vehicle;**
- .5 deny access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and**
- .6 using of patrol vessels to enhance waterside security.**

Security Level 3

16.20 At security level 3, the port facility should comply with instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 suspension of access to all, or part of, the port facility;
- .2 granting access only to those responding to the security incident or threat thereof;
- .3 suspension of pedestrian or vehicular movement within all, or part, of the port facility;
- .4 increased security patrols within the port facility, if appropriate;
- .5 suspension of port operations within all, or part, of the port facility;
- .6 direction of vessel movements relating to all, or part, of the port facility; and
- .7 evacuation of all, or part of, the port facility.

Restricted areas within the port facility

16.21 The PFSP should identify the restricted areas to be established within the port facility, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. This should also include, in appropriate circumstances, measures to ensure that temporary

restricted areas are security swept both before and after that area is established. The purpose of restricted areas is to:

- .1 protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;**
- .2 protect the port facility;**
- .3 protect ships using, and serving, the port facility;**
- .4 protect sensitive security locations and areas within the port facility;**
- .5 to protect security and surveillance equipment and systems; and**
- .6 protect cargo and ship's stores from tampering.**

16.22 *The PFSP should ensure that all restricted areas have clearly established security measures to control:*

- .1 access by individuals;**
- .2 the entry, parking, loading and unloading of vehicles;**
- .3 movement and storage of cargo and ship's stores; and**
- .4 unaccompanied baggage or personal effects.**

16.23 *The PFSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.*

16.24 *When automatic intrusion detection devices are installed they should alert a control centre which can respond to the triggering of an alarm.*

16.25 *Restricted areas may include:*

- .1 shore and waterside areas immediately adjacent to the ship;**
- .2 embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas including search points;**
- .3 areas where loading, unloading or storage of cargo and stores is undertaken;**
- .4 locations where security sensitive information, including cargo documentation, is held;**
- .5 areas where dangerous goods and hazardous substances are held;**
- .6 vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;**
- .7 areas where security and surveillance equipment are stored or located;**
- .8 essential electrical, radio and telecommunication, water and other utility installations; and**
- .9 other locations in the port facility where access by vessels, vehicles and individuals should be restricted.**

16.26 The security measures may extend, with the agreement of the relevant authorities, to restrictions on unauthorized access to structures from which the port facility can be observed.

Security Level 1

16.27 At security level 1, the PFSP should establish the security measures to be applied to restricted areas, which may include:

- .1 provision of permanent or temporary barriers to surround the restricted area whose standard should be accepted by the Contracting Government;**
- .2 provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;**
- .3 providing passes which must be displayed to identify individuals entitlement to be within the restricted area;**
- .4 clearly marking vehicles allowed access to restricted areas;**
- .5 providing guards and patrols;**
- .6 providing automatic intrusion detection devices, or surveillance equipment or systems to detect unauthorized access into, or movement within restricted areas; and**
- .7 control of the movement of vessels in the vicinity of ships using the port facility.**

Security Level 2

16.28 At security level 2, the PFSP should establish the enhancement of the frequency and intensity of the monitoring of, and control of access to, restricted areas. The PFSP should establish the additional security measures, which may include:

- .1 enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion detection devices;**
- .2 reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;**
- .3 restrictions on parking adjacent to berthed ships;**

- .4 further restricting access to the restricted areas and movements and storage within them;**
- .5 use of continuously monitored and recording surveillance equipment;**
- .6 enhancing the number and frequency of patrols including waterside patrols undertaken on the boundaries of the restricted areas and within the areas;**
- .7 establishing and restricting access to areas adjacent to the restricted areas; and**
- .8 enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility.**

Security Level 3

16.29 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied; and**
- .2 preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.**

Handling of cargo

16.30 The security measures relating to cargo handling should:

- .1 prevent tampering; and**
- .2 prevent cargo that is not meant for carriage from being accepted and stored within the port facility.**

16.31 The security measures should include inventory control procedures at access points to the port facility. Once within the port facility cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary

storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

Security Level 1

16.32 *At security level 1, the PFSP should establish the security measures to be applied during cargo handling, which may include:*

- .1** routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;
- .2** checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;
- .3** searches of vehicles; and
- .4** checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

16.33 Checking of cargo may be accomplished by some or all of the following means:

- .1** visual and physical examination; and
- .2** using scanning/detection equipment, mechanical devices, or dogs.

16.34 When there are regular, or repeated, cargo movement the Company Security Officer (CSO) or the Ship Security Officer (SSO) may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSP concerned.

Security Level 2

16.35 *At security level 2, the PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include:*

- .1 detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;**
- .2 intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship;
- .3 intensified searches of vehicles; and
- .4 increased frequency and detail in checking of seals and other methods used to prevent tampering.

16.36 Detailed checking of cargo may be accomplished by some or all of the following means:

- .1 increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination);
- .2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and
- .3 co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security Level 3

16.37 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 *restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and***
- .2 verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.

Delivery of ship's stores

16.38 *The security measures relating to the delivery of ship's stores should:*

- .1 ensure checking of ship's stores and package integrity;
- .2 prevent ship's stores from being accepted without inspection;
- .3 prevent tampering;
- .4 prevent ship's stores from being accepted unless ordered;
- .5 ensure searching the delivery vehicle; and
- .6 ensure escorting delivery vehicles within the port facility.

16.39 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

16.40 At security level 1, the PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include:

- .1 *checking of ship's stores;*
- .2 *advance notification as to composition of load, driver details and vehicle registration; and*
- .3 searching the delivery vehicle.

16.41 Checking of ship's stores may be accomplished by some or all of the following means:

- .1 visual and physical examination; and
- .2 using scanning/ detection equipment, mechanical devices or dogs.

Security Level 2

16.42 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ship's stores, which may include:

- .1 detailed checking of ship's stores;
- .2 detailed searches of the delivery vehicles;
- .3 co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; and
- .4 escorting the delivery vehicle within the port facility.

16.43 Detailed checking of ship's stores may be accomplished by some or all of the following means:

- .1 increasing the frequency and detail of searches of delivery vehicles;
- .2 increasing the use of scanning/ detection equipment, mechanical devices, or dogs; and
- .3 restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period.

Security Level 3

16.44 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility which may include preparation for restriction, or suspension, of the delivery of ship's stores within all, or part, of the port facility.

Handling unaccompanied baggage

16.45 The PFSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before is allowed in the port facility and, depending on the storage arrangements, before it is transferred between the port facility and the ship. It is not envisaged that such baggage will be subjected to screening by both the port facility and the ship, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the ship is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

16.46 At security level 1, the PFSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

16.47 At security level 2, the PFSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

16.48 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;*
- .2 preparations for restriction or suspension of handling of unaccompanied baggage; and*
- .3 refusal to accept unaccompanied baggage into the port facility.*

Monitoring the security of the port facility

16.49 *The port facility security organization should have the capability to monitor the port facility and its nearby approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:*

- .1 lighting;**
- .2 security guards, including foot, vehicle and waterborne patrols; and**

- .3 automatic intrusion detection devices and surveillance equipment.**

16.50 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

16.51 The PFSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or of power disruptions.

Security Level 1

16.52 At security level 1, the PFSP should establish the security measures to be applied which may be a combination of lighting, security guards or use of security and surveillance equipment to allow port facility security personnel to:

- .1 observe the general port facility area, including shore and water-side accesses to it;**
- .2 observe access points, barriers and restricted areas; and**
- .3 allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself.**

Security Level 2

16.53 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capability, which may include:

- .1 increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage;**
- .2 increasing the frequency of foot, vehicle or waterborne patrols; and**
- .3 assigning additional security personnel to monitor and patrol.**

Security Level 3

16.54 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 switching on all lighting within, or illuminating the vicinity of, the port facility;
- .2 switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and
- .3 maximising the length of time such surveillance equipment can continue to record.

Differing security levels

16.55 *The PFSP should establish details of the procedures and security measures the port facility could adopt if the port facility is at a lower security level than that applying to a ship.*

Activities not covered by the Code

16.56 *The PFSP should establish details of the procedures and security measures the port facility should apply when:*

- .1 it is interfacing with a ship which has been at a port of a State which not a Contracting Government;*
- .2 it is interfacing with a ship to which this Code does not apply; and*
- .3 it is interfacing with fixed or floating platforms or mobile offshore drilling units on location.*

Declarations of security

16.57 *The PFSP should establish the procedures to be followed when on the instructions of the Contracting Government the PFSO requests a Declaration of Security or when a DoS is requested by a ship.*

Audit, review and amendment

16.58 *The PFSP should establish how the PFSO intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP.*

16.59 The PFSP should be reviewed at the discretion of the PFSO. In addition it should be reviewed:

- .1 if the PFSA relating to the port facility is altered;
- .2 if an independent audit of the PFSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant element of the approved PFSP;
- .3 following security incidents or threats thereof involving the port facility; and
- .4 following changes in ownership or operational control of the port facility.

16.60 The PFSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the PFSP relating to:

- .1 proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; and
- .2 the removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems etc., previously considered essential in maintaining the security of the port facility;

should be submitted to the Contracting Government that approved the original PFSP for their consideration and approval. Such approval can be given by, or on behalf of, the Contracting Government with, or without, amendments to the proposed changes. On approval of the PFSP the Contracting Government should indicate which procedural or physical alterations have to be submitted to it for approval.

Approval of port facility security plans

16.61 *PFSPs have to be approved by the relevant Contracting Government which should establish appropriate procedures to provide for:*

- .1 the submission of PFSPs to them;**
- .2 the consideration of PFSPs;**
- .3 the approval of PFSPs, with or without amendments;**
- .4 consideration of amendments submitted after approval; and**
- .5 procedures for inspecting or auditing the continuing relevance of the approved PFSP.**

At all stages steps should be taken to ensure that the contents of the PFSP remains confidential.

Statement of Compliance of a Port Facility

16.62 The Contracting Government within whose territory a port facility is located may issue an appropriate Statement of Compliance of a Port Facility (SoCPF) indicating:

- .1 the port facility;**
- .2 that the port facility complies with the provisions of chapter XI-2 and part A of the Code;**
- .3 the period of validity of the SoCPF which should be specified by the Contracting Governments but should not exceed five years; and**
- .4 the subsequent verification arrangements established by the Contracting Government and a confirmation when these are carried out.**

16.63 The Statement of Compliance of a Port Facility should be in the form set out in the appendix to this Part of the Code. If the language used is not Spanish, French or English, the Contracting Government, if it considers it appropriate, may also include a translation into one of these languages.

17 PORT FACILITY SECURITY OFFICER

General

17.1 In those exceptional instances where the ship security officer has questions about the validity of identification documents of those seeking to board the ship for official purposes, the port facility security officer should assist.

17.2 The port facility security officer should not be responsible for routine confirmation of the identity of those seeking to board the ship.

In addition other relevant guidance is provided under sections 15, 16 and 18.

18 TRAINING, DRILLS AND EXERCISES ON PORT FACILITY SECURITY

Training

18.1 *The Port Facility Security Officer should have knowledge and receive training, in some or all of the following, as appropriate:*

- .1 security administration;**
- .2 relevant international conventions, codes and recommendations;**
- .3 relevant Government legislation and regulations;**
- .4 responsibilities and functions of other security organizations;**
- .5 methodology of port facility security assessment;**
- .6 methods of ship and port facility security surveys and inspections;**
- .7 ship and port operations and conditions;**
- .8 ship and port facility security measures;**
- .9 emergency preparedness and response and contingency planning;**
- .10 instruction techniques for security training and education, including security measures and procedures;**
- .11 handling sensitive security related information and security related communications;**
- .12 knowledge of current security threats and patterns;**
- .13 recognition and detection of weapons, dangerous substances and devices;**

- .14 recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;**
- .15 techniques used to circumvent security measures;
- .16 security equipment and systems, and their operational limitations;
- .17 methods of conducting audits, inspection, control and monitoring;**
- .18 methods of physical searches and non-intrusive inspections;**
- .19 security drills and exercises, including drills and exercises with ships; and
- .20 assessment of security drills and exercises.**

18.2 *Port facility personnel having specific security duties should have knowledge and receive training, in some or all of the following, as appropriate:*

- .1 knowledge of current security threats and patterns;
- .2 recognition and detection of weapons, dangerous substances and devices;
- .3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;**
- .4 techniques used to circumvent security measures;
- .5 crowd management and control techniques;
- .6 security related communications;
- .7 operations of security equipment and systems;
- .8 testing, calibration and maintenance of security equipment and systems;
- .9 inspection, control, and monitoring techniques; and**
- .10 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.**

18.3 *All other port facility personnel should have knowledge of and be familiar with relevant provisions of the PFSP, in some or all of the following, as appropriate:*

- .1 the meaning and the consequential requirements of the different security levels;

- .2 recognition and detection of weapons, dangerous substances and devices;
- .3 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and**
- .4 techniques used to circumvent security measures.

Drills and exercises

18.4 The objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties, at all security levels, and to identify any security related deficiencies, which need to be addressed.

18.5 To ensure the effective implementation of the provisions of the port facility security plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as those security threats listed in paragraph 15.11.

18.6 Various types of exercises which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, company security officers, or ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of company security officers or ships security officers in joint exercises should be made bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response. These exercises may be:

- .1 full scale or live;
- .2 tabletop simulation or seminar; or
- .3 combined with other exercises held such as emergency response or other port State authority exercises.

19 VERIFICATION AND CERTIFICATION OF SHIPS

No additional guidance.

APPENDIX TO PART B

APPENDIX 1

Form of a Declaration of Security between a ship and a port facility²⁵

DECLARATION OF SECURITY

Name of Ship:	
Port of Registry:	
IMO Number:	
Name of Port Facility:	

This Declaration of Security is valid from until, for the following activities

.....
(list the activities with relevant details)

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by		
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing		

²⁵ This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two ships this model should be appropriately modified.

areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated aton the

Signed for and on behalf of	
the port facility:	the ship:

(Signature of Port Facility Security Officer)

(Signature of Master or Ship Security Officer)

Name and title of person who signed	
Name:	Name:
Title :	Title :

Contact Details <i>(to be completed as appropriate)</i> <i>(indicate the telephone numbers or the radio channels or frequencies to be used)</i>	
for the port facility:	for the ship:

Port Facility

Master

Port Facility Security Officer

Ship Security Officer

Company

Company Security Officer

APPENDIX 2

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

(Official seal)

(State)

Statement Number

**Issued under the provisions of Part B of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)**

The Government of _____
(name of the State)

Name of the Port Facility :
Address of the Port Facility :

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Port Facility Security Plan. This plan has been approved for the following <specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):

Passenger ship

Passenger high speed craft

Cargo high speed craft

Bulk carrier

Oil tanker

Chemical tanker

Gas carrier

Mobile offshore Drilling Units

Cargo ships other than those referred to above

This Statement of Compliance is valid until, subject to verifications (as indicated overleaf)

Issued at.....
(place of issue of the statement)

Date of issue.....
(Signature of the duly authorized official)

issuing the document)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR VERIFICATIONS

The Government of *<insert name of the State>* has established that the validity of this Statement of Compliance is subject to *<insert relevant details of the verifications (e.g. mandatory annual or unscheduled)>*.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

1st VERIFICATION

Signed:
(Signature of authorized official)

Place:

Date:

2nd VERIFICATION

Signed:
(Signature of authorized official)

Place:

Date:

3rd VERIFICATION

Signed:
(Signature of authorized official)

Place:

Date:

4th VERIFICATION

Signed:
(Signature of authorized official)

Place:

Date:

THE MINISTRY OF FOREIGN AFFAIRS

On the basis of Article 26. and Article 30. paragraph 3. of the Law on Conclusion and Execution of International Agreements ("Narodne novine", No. 28/96), the Ministry of Foreign Affairs of the Republic of Croatia

ANNOUNCES

that the Amendments to the Annex to the 1974 Convention for the Safety of Life at Sea, published in "Narodne Novine - International Agreements" No. XX/YY, and the International Code for the Security of Ships and of Port Facilities (ISPS), published in "Narodne Novine - International Agreements" No. XX/YY, that were adopted at the Diplomatic Conference of the International Maritime Organisation on Maritime Security, held in London from 9th to 13th December 2002, entered into force on 1st July 2004 following the tacit amendment procedure adopted in the 1974 Convention for the Safety of Life at Sea.

Class: XXX-XX/XX-XX/XX

Reg. Number: XXX-XX-XX-XX/XX-XX-XX

Zagreb, dd. July 2004.

The Minister of Foreign Affairs