REPUBLIC OF CYPRUS

MINISTRY OF COMMUNICATIONS AND WORKS
DEPARTMENT OF MERCHANT SHIPPING
LEMESOS

Circular No: 14/2003

TEN 1/5
TEN 32/5/1/42/1

02 October 2003

To all Owners, Managers
and Representatives of
ships flying the Cyprus flag

Subject: Special Measures to Enhance Maritime Security
Implementation of Chapter XI-2 of SOLAS 74 as amended and the ISPS Code

0 Introduction

0.1 The Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as amended, which was held in London between the 9 and 13 December 2002, adopted a number of amendments to the International Convention for the Safety of Life at Sea, 1974 as amended (SOLAS 74) and the International Code for the Security of Ships and of Port Facilities (ISPS Code) for the purpose of enhancing security in the international maritime transport sector.

0.2 In the light of the political climate under which the measures to enhance maritime security were developed and adopted, it is highly unlikely that any of the Contracting Governments to SOLAS 74 (Contracting Governments) will invoke the provisions of Article VIII(b)(vi) of SOLAS 74 and object to the amendment. In addition, it is not anticipated that any of the Contracting Governments will invoke the provisions of Article VIII(b)(vii) and give notice that it exempts itself from giving effect to the amendments. Thus the amendments to SOLAS 74 will enter into force on the 1 July 2004.

1 Purpose of this circular

1.1 The purpose of this circular is not to analyse the recently adopted amendments to SOLAS 74 (the amendments) or the ISPS Code[1]. In view of the limited time between now and the entry into force of the amendments, this circular is intended to provide those concerned with guidance and advice so as to enable them to make the necessary arrangements to ensure, on time, prompt and completed compliance.

1.2 The present circular addresses various aspects relating to the amendments as well as various questions be raised those concerned, so far, with the Department and provides the orientation of the Department on various aspects relating to the amendments and the ISPS Code.

[1] The International Maritime Organisation has already published the amendments and the ISPS Code in a single publication (ISPS Code 2003 Edition) the sale number of which is 116E.

1.3 This circular will be followed, during the next few weeks, by a further advice and guidance in the areas which are specified in this circular, as well as, on the European Union legislation (see below) in the area of ship and port facility security.

1.4 In case the Department receives any requests for further advice or guidance, the various answers, if these relate to issues of general interest, will be consolidated from time to time and issued in the form of a circular supplementing the present one.

1.5 However, the Department strongly urges all parties concerned to start making the necessary arrangements NOW and NOT to wait any longer.

1.6 It should be noted that the present circular addresses ships and does not cover port facilities.

2 Expected European Union legislation

2.1 The draft of a proposed Regulation of the European Parliament and of the Council on enhancing ship and port facility security is at an advanced stage (the draft EU Regulation).

2.2 The main objective of the draft EU Regulation is to introduce and implement European Community measures aimed at enhancing the security of ships used in either international trade or domestic shipping and associated port facilities in the face of threats of intentional unlawful acts.

2.3 The draft EU Regulation is also intended to provide a basis for harmonised interpretation and implementation and European Community monitoring of the special measures to enhance maritime security contained in chapter XI-2 of SOLAS 74 and in the ISPS Code.

2.4 This legislation will be applicable to Cyprus and will also apply to ships, irrespective of the flag they are flying, visiting port facilities located within the territory of the Members of the European Union and of the Members of the European Economic Area.

3 Some background information

3.1 Although the work within the International Maritime Organisation (IMO) was initiated as a result of the "9/11 events" the outcomes (i.e. the amendments) address all aspects of security in the international maritime transport sector.

3.2 In this respect, attention is drawn to the definition of security incident (Regulation[2] XI-2/1.13 - Definitions) which provides that *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[3] or of any ship/port interface[4] or any ship-to-ship activity[5].*

[2] Any reference, in this circular, to "chapter" or "regulation", unless indicated otherwise, is a reference to a chapter or regulation of SOLAS 74.
[3] Defined in regulation XI-2/1.9.
[4] Defined in regulation XI-2/1.8.
[5] Defined in regulation XI-2/1.10.

3.3 Thus, in simple terms, the recently adopted measures address a range of security incidents from thefts, unauthorised access, stowaways, illegal migrants, piracy, armed robbery and acts of terrorism.

3.4 The measures aim towards establishing a security conscious culture amongst seafarers, ship owners, ship operators, maritime sector services providers and port facility operators, users and services providers and focus on enhancing awareness and vigilance.

3.5 It is noted that the measures to enhance maritime security are calling for the establishment of appropriate operational measures and procedures to prevent unauthorized access, to prevent the introduction of unauthorised weapons, incendiary devices or explosives, to provide means of raising an alarm, to ensure efficient and effective communications and to enhance awareness and vigilance.

3.6 These measures have a protective character and have been developed for the purpose of preventing the occurrence of a security incident.

3.7 Suppression, containment and control of a situation in case of breach of security or of a security incident, has been and remains a matter for the police and the security services of each State.

3.8 It is advisable, when reading the recently adopted measures to enhance maritime security, to bear in mind that a ship may be:

- used as a weapon;
- used as a means for transporting either persons intending to cause a security incident or their means, such as weapons or other dangerous substances or devices or parts thereof, for such incident; and
- used in a lawful trade for the purpose of generating funds to finance terrorist activities.

3.9 The recently adopted measures address the first two aspects. The third one, i.e. the use of a ship in a lawful trade for the purpose of generating funds to finance terrorist activities, is not explicitly or directly addressed. However, a provision has been made, in this respect, for ships (see regulation XI-2/5 – Specific responsibility of Companies) to carry on board various documentary evidence attesting the employment of the ship (i.e. who decides the chartering and who are the charterers) and the employment of the seafarers working on board. These are to be made available to the competent authorities of each State, which is Contracting Government, for the "investigative" work of their security services.

3.10 During the discussion at IMO it was recognised and accepted that what is or constitutes a security threat and what is a security risk, is a matter which falls within the competency of the security services of each State and, in this respect, only indicative examples have been included in Part B of the ISPS Code which has a recommendatory character.

3.11 How these services operate or co-operate with their counterparts in other States remains classified and is the prerogative of the States concerned. Due care has been taken not to touch this issue.

3.12 When carrying ship security surveys or inspections, when preparing ship security assessments (SSA), when designing security measures and procedures, when developing ship security plans (SSP) and when implementing, maintaining, reviewing and revising security measures, it is recommended to bear in mind the objectives (section[6] A/1.2 – Objectives), the functional requirements (section A/1.3 – Functional requirements) the ship security activities (section A/7.2 – Ship security) and the port facility security activities (section A/14.2 – Port facility security).

3.13 It is furthermore noted that the implementation of these measures should not necessarily entail structural modifications to the ships which will be in service on the 1 July 2004. However, ships may be required, as a result of the ship's security assessment, to carry out minor structural work (e.g. fitting locks, motion sensors, close television cameras, low lighting cameras, additional lighting, barriers or providing security equipment such as for example metal detectors or scanners) in order to meet the requirements of ISPS Code in an optimal manner.

4 Part B of the ISPS Code

4.1 Part B of the ISPS Code has a recommendatory character and has been developed for the purpose of enabling those concerned to meet the requirements of chapter XI-2 and Part A of the ISPS Code.

4.2 It is understood that a number of Contracting Governments are considering making compliance with certain paragraphs of Part B of the ISPS Code mandatory for ships entitled to fly their flag and for all ships visiting port facilities located within their territory.

4.3 Realistically speaking the provisions of , Part B of the ISPS Code constitute an essential guidance in the process of preparing a SSA, designing security measures and procedures, developing a SSP and implementing, maintaining, reviewing and revising security measures.

4.4 The Maritime Safety Committee of IMO, at its seventy-seventh session, issued MSC/Circ. 1097, copy of which is attached, on Guidelines Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code which states:

> *"8 The Committee recognized that part B of the ISPS Code was albeit recommendatory, a process all parties concerned needed to go through in order to comply with part A. It was concluded that paragraph 9.4 of part A of the ISPS Code required that in order for an ISSC to be issued, the guidance in part B would need to be taken into account.*
>
> *9 The Committee further specifically considered that an ISSC would not be issued unless paragraphs 8.1 to 13.8 of part B of the ISPS Code had been taken into account."*

4.5 The current draft EU Regulation specifies that the following paragraphs of Part B of the ISPS Code, relating to ships, will be mandatory:

[6] Any reference, in this circular, to "section", unless indicated otherwise, is a reference to section of Part A of the ISPS Code and is indicated as "section A/<followed by the section number>".

"▪ *1.12 (revision of ship security plans),*
- *4.1 (protection of the confidentiality of security plans and assessments),*
- *4.4 (recognised security organisation),*
- *4.5 (minimum competencies of recognised security organisations),*
- *4.8 (setting the security level),*
- *4.14, 4.15, 4.16 (contact points and information on port facility security plans),*
- *4.18 (identification documents),*
- *4.24 (ships' application of the security measures recommended by the State in whose territorial waters they are sailing),*
- *4.28 (manning level),*
- *4.41 (communication of information when entry into port is denied or the ship is expelled from port),*
- *4.45 (ships from a State which is not party to the Convention),*
- *6.1 (company's obligation to provide the master with information on the ship's operators),*
- *8.3 to 8.10 (minimum standards for the ship security assessment),*
- *9.2 (minimum standards for the ship security plan),*
- *9.4 (independence of recognised security organisations),*
- *13.6 and 13.7 (frequency of security drills and exercises for ships' crews and for company and ship security officers)"*

4.6 However, meticulous adherence to the guidance provided in Part B of the ISPS Code may be not enough to achieve the objective of enhancing security in the international maritime transport sector.

4.7 Those concerned, if they wish to be effective and proactive and as we are dealing with security aspects where the unexpected is the rule and the element of surprise is the key to success, should NOT limit themselves to the guidance provided in Part B of the ISPS Code.

4.8 It is strongly recommended that all aspects should be considered however remote they might be. Nevertheless, in the interest of maintaining and facilitating efficient international trade, "worst case scenarios" may not necessarily be the route and the key to success. Whatever scenarios are used in the development, implementation and maintenance of security measures, MUST ALWAYS be supplemented by continuous enhancement of awareness and vigilance and an ongoing proactive and adaptive attitude.

5 Application to ships

5.1 Regulation XI-2/2.1.1 (and section A/3.1.1) indicates that the measures to enhance maritime security apply to the following types of ships engaged in 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.

5.2 With respect to ships, as a rough guide, any ship which is required to hold a valid Passenger Ship Safety Certificate, Cargo Ship Safety Construction or Equipment Certificate, Passenger or Cargo High Speed Craft Certificate and mechanically

propelled mobile offshore drilling units when not on location, are required to comply with the requirements of chapter XI-2 and Part A of the ISPS Code.

5.3 In addition, any Company (as defined in regulations XI-2/1.7 and IX/1) operating a ship (including mechanically propelled mobile offshore drilling unit when not on location) to which chapter XI-2 and part A of the ISPS Code apply, is required to comply (regulation XI-2/4.1) with the requirements of chapter XI-2 and Part A of the ISPS Code.
Again, as a rough guide, any Company which is required to hold a valid Document of Compliance is required to comply with chapter XI-2 and Part A of the ISPS Code.

6 Identification of the Company

6.1 Unless the Department is advised otherwise, not later than the 30 June 2004,the Government of the Republic of Cyprus will consider that, for all ships which will be flying the flag of the Republic of Cyprus on the 1 July 2004,their registered owners (or their registered bareboat charterers) and the Company which operates each of these ships accept and agree that the Company, as notified to the Department on the basis of the Department's circular letter 13/2002 for the purpose of compliance with the requirements of chapter IX and the ISM Code, undertakes to carry out and perform all duties and responsibilities of the Company under chapter XI-2 and the ISPS Code.

6.2 The Department is in the process of revising parts of its circular letter 13/2002 and some of the associated notification forms, so as to incorporate the necessary changes to reflect the needs arising from chapter XI-2 and the ISPS Code.

7 Ship Security Assessments

Sister ships

7.1 The Department is willing to consider, on a case by case basis, (subject to the provisions of the draft EU Regulation) requests for allowing a single Ship Security Assessment for physically identical sister ships operating on the same routes (i.e. exposed to identical security threats) and having the same complement in terms of shipboard personnel, provided these assessments, when submitted with the associated Ship Security Plans are accompanied by the on scene security survey , through which the validity of the assessment is attested for each of the sister ships, subject to a physical check by the surveyor.

8 Ship Security Plans

General

8.1 A number of Companies and ships have already in place various measures, procedures or policies, as part of either a quality system, or their safety management system, or as a good practice, relating to various aspects of to security such as, for example, access of visitors, stowaways, piracy and armed robbery or drugs and alcohol.

8.2 It is recommended, in view of the familiarity of the shipboard personnel with these measures, procedures or policies, to continue these and use them in the development of the SSP. However, if these are to be used, they should be reviewed, revised and amended to reflect the requirements of chapter XI-2 and Part A of the ISPS Code and should be incorporated in the SSP.

In case the Company wishes, bearing in mind the provisions of section A/9.8 and A/9.8.1, to retain them as a part of their quality or safety management systems, or as a good practice (i.e. as a non confidential document protected from unauthorised access or disclosure) these should be consistent with those to be included in the SSP.

8.3 Annex 1 addresses, amongst others, the questions "who prepares the SSP" and "who approves the SSP".

Copies of the approved SSP and of any subsequent amendments thereto

8.4 When preparing the number of copies of the SSP to be submitted for review and approval (or any subsequent amendments to a previously approved plan) it should be noted that the Department requires each Company to have in the office from which the ship is operated at least one copy of the approved SSP (including any subsequently approved amendments thereto) relating to that ship. This copy of the SSP (and any amendments thereto) shall be protected from unauthorised access or disclosure.

8.5 The draft EU Regulation provides, as a part of the implementation and conformity checking process, that the European Commission will carry out inspections, including inspections of a suitable sample of port facilities and of Companies, to monitor the application of the regulation by Member States.
Therefore, Companies are required to have at their offices, in addition to the copy of the approved SSP (including any subsequent approved amendments thereto), as indicated above, documentary evidence attesting that the Company discharges all its obligation under the provisions of chapter XI-2, the ISPS Code, the draft EU Regulation and the provisions of the approved SSP.
Failure to meet this requirement, including the requirement to have a copy of the approved SSP, will be considered as a failure of the Company to meet its obligations under chapter XI-2, the ISPS Code and the draft EU Regulation.

The format of the SSP

8.6 The ISPS Code specifies the elements to be included in the SSP. Neither the ISPS Code nor any other IMO document, at present, specifies the format or the layout of the SSP. In addition so far no specific proposal has been made for IMO to determine a specific format or layout of the SSP.

8.7 It is not envisaged that the Department would require a specific format or layout. Furthermore the Department will not reject it is not our intention to require any specific format or layout which any Recognised Security Organisation (RSO) may suggest or stipulate. Should those concerned decide to follow a specific format or layout an RSO may suggest or stipulate, the Department will accept it.

8.8 The important aspect is for the SSP to contain all the elements which Parts A and B of the ISPS Code specify. It will be useful for the SSP to be a controlled document and to contain a table of contents through which the various elements, measures and procedures can be easily identified.

8.9 It is advisable that the SSP is structured with the user in mind, in a similar manner as other shipboard plans (such as for example, the Shipboard Oil Emergency Response Plan (SOPEP)and the Garbage Management Plan) already provided on board.

Ship Security Plan as part of the Safety Management System

8.10 A review of the work of IMO relating to the development of the ISPS Code shows that the possibility of combining the ship´s SSP with the ship's safety management system was considered. However, for various reasons, mostly associated

with aspects of national security and the need to protect the SSP from unauthorised access and disclosure, the Contracting Governments decided not to allow this option.

8.11 In fact, section A/9.8 specifies that the SSPs 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* A/ 9.8.1.
Section A/9.8.1 states that, 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.*

8.12 In the light of the aforesaid and in the interest of the national security of the Republic of Cyprus as well as of the other Contracting Governments, SSPs shall NOT form or be part of safety management systems.

The development of SSPs and the Control and Compliance Measures

8.13 The Department strongly recommends that those involved with the development of a SSP undertake a comprehensive study of the provisions of regulation XI-2/9 on Control and Compliance Measures and of the associated paragraphs B/4.29 to B/4.46. In addition, the Department recommends that those concerned with this task, undertake a review of the information and guidance published by Contracting Governments for foreign ships calling at their ports.

9 Security equipment

9.1 It is not anticipated that the department require specific security equipment to be provided on board ships flying the flag of the Republic of Cyprus.

9.2 The need and the type and nature of any security equipment to be provided on board, will be one of the outcomes of the SSA and the process of designing the security measures and procedures to be implemented on board.

9.3 The SSP shall identify any security equipment which is provided on board, as apart of the process of complying and maintaining compliance with the requirements of chapter XI-2 and Part A of the ISPS Code.
The SSP shall also indicate any replacement security equipment, or part thereof and the spares which need to be available on board (e.g. when security equipment is sent ashore for repairs or maintenance, or need, to be replaced by the ship´s personnel as a result of malfunctioning or failure) so as to ensure that the necessary security equipment is available on board in a functional condition at all times.

9.4 As a plethora of security equipment is available in the market, we expect those concerned to ensure, when selecting the security equipment to be provided, that it is suitable for use in the marine environment and can withstand the humidity, the salinity, the temperature, the vibration and the acceleration range and in case of ships carrying flammable liquids or gases, it is explosion proof.

9.5 The suitability of any security equipment will be considered at the stage of review and approval of the SSP (or of any subsequent amendments to the SSP). The

availability (or installation) on board of any security equipment, its efficient functioning and the familiarity of the shipboard personnel with its use, operational limitations and the manufacturers, requirements regarding maintenance, calibration and testing will be checked during the initial verification process (and subsequent verifications) for the issue (or endorsement) of the International Ship Security Certificate (or the issue of an Interim International Ship Security Certificate).

10 Company Security Officers

10.1 The Company, bearing in mind sections A/11.2, A/13.1 and paragraph B/13.1, shall designate Company Security Officer(s) (CSO(s)) for the ships it operates[7].

10.2 The Company, bearing in mind sections A/11.2, A/13.1 and paragraph B/13.1, shall also designate alternate CSOs and their names and contact details shall be identified in the SSP.

10.2.1 The principle to be observed is that, at all times a person shall be available ashore who can carry out and perform the duties and responsibilities of the CSO, under Part A of the ISPS Code.

10.3 Any Designated Persons (DP) (section 4 of the ISM Code) and any alternate DP, may also be designated as a CSO or alternate CSO, provided the requirements of sections A/11.2, A/13.1 and paragraph B/13.1 are met. In such a case, it is the Company concerned which has to ensure that such a person can adequately and efficiently perform both functions.

10.4 For all ships, which on the 1 July 2004 will be flying the flag of the Republic of Cyprus, the name and contact details[8] (including contact details outside office hours) of the CSO and of the alternate CSO shall be communicated to the Department not later than the 1 July 2004.

10.5 The Department shall also forthwith be advised on any subsequent changes (i.e. changes of names or of contact details) relating to the CSO or the alternate CSO.

10.6 The Department is in the process of preparing and making available for use, a standardised form for communicating the name and contact details of the CSO and of the alternated CSO and any changes relating thereto.

11 Ship Security Officers

11.1 The Company, bearing in mind section A/12.2, A/13.2 and paragraph B/13.2, shall designate a Ship Security Officer (SSO) for each of the ships it operates.

11.2 For each ship the Company shall designate also an alternate SSO who shall be identified in the SSP.

---

[7] Section A/11.1 states that 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.*

[8] For the purpose of enabling expedient and efficient communications, the Department will highly appreciated it to receive the e-mail addresses of the CSO and the alternate CSO, where available, together with an indication whether these can be used for secure communications (i.e. the transmission of security related information).

11.2.1 The principle to be observed is that at all times a person shall be available onboard who can carry out and perform the duties and responsibilities, under Part A of the ISPS Code, of the SSO (i.e. in case of shore leave of the SSO or in case the SSO has to go ashore for medical care or for the business of the ship or in case the SSO has departed and the replacement SSO has not yet arrived).

11.3 Any member of the ship's personnel, including the Master, may be designated as the SSO or as an alternate SSO, provided he has the required training and understanding of the duties and obligations of the SSO or of the alternate SSO.

11.4 The nature of the duties and responsibilities of the SSO and of the alternate SSO, particularly the ones relating to access to the ship by persons, including their carry on items and security aspects relating to passengers, cargo, ship's stores and unaccompanied baggage, indicate that the person to be designated to such duties is required to have the necessary level of authority, a broad understanding of and involvement in the day-to-day operations of the ship and be available on board at all times.

11.5 In case a Company decides to designate an engineer officer as either an SSO or an alternate SSO, the Company must ensure that, in matters relating to security, his overriding authority to intervene and give directions in areas other than those which normally fall within the engine department, is clearly and unambiguously stated in the SSP. In addition, the SSP should clearly indicate the arrangements which immediately have to be put in place in case it is required, during any periods of his engagement in watch-keeping or machinery spaces duties, to enable him to attend any security related issues outside the machinery spaces.

11.6 The SSO and the alternate SSO may be identified, in the SSP, by reference to the rank of the persons on board (e.g. the SSO is the Chief Officer and the alternate SSO is the Second Officer). Entry of the actual name of the SSO or alternate SSO in the SSP is not required. In this way the SSO and the alternate SSO will be identified through a cross reference to the Crew List of the ship at the time. In this manner, the need to submit amendments to the SSP for approval, as a result of shipboard personnel changes, will be avoided.

11.7In the case of passenger ships, the SSO and the alternate SSO need not be member of the deck or engine room shipboard personnel and may be persons specialised in security. In such case the persons to be designated as SSO and as alternate SSO, in addition to the requirements of section A/13.2 and paragraph B/13.2, shall meet the requirements of regulation VI/1 of STCW 78 as amended and section A-V/1 of the STCW Code.

11.8 The Department does not anticipate that any form of additional (external) verification will be required when the SSO or the alternate SSO are replaced.
However, Companies shall address this issue in the SSP and provide specific procedures in this respect, so that it may be considered during subsequent verifications.
In addition, the Company shall verify, during the internal audits of the SSP that these procedures have been observed.

12 Records

General

12.1 The amendments to SOLAS 74 and the ISPS Code specify the documentary evidence, information and records which need to be available or kept. These are:

(1) the documentary evidence referred to in regulation XI-2/5 – Specific responsibility of Companies and paragraph B/6;

(2) the information referred to in regulation XI-2/9.2.1;

(2) the records in connection with activities addressed in the SSP referred to in section A/10 – Records and paragraph B/10;

(3) the Declarations of Security referred to in section A/5 and paragraph B/5.

12.2 In general, all required documentary evidence, information, records and Declarations of Security (collectively referred to as "documentary material") have to be kept for a period not less than 5 years or until the completion of the subsequent renewal verification, whichever of the two occurs the last.

12.3 In addition, any of the aforesaid documentary material which relate to any proceedings (e.g. control and compliance proceedings, administrative or legal proceedings), in case they fall under the above principle, have to be kept until the proceedings in question (and any appeal proceedings relating thereto) are completed.

12.4 The Company and the ship, where appropriate, shall retain records(including information such as what, when, where, witnesses……) showing that specific documentary materials, the further keeping of which was not longer necessary, have been physically destroyed or, in case of electronic records, that they have been deleted and their recovery is not physically possible.

12.5 All documentary material shall be treated as confidential and shall be protected from unauthorised access and disclosure.

Documentary materials and SSPs

12.6 The Department is presently considering its approach on the aforesaid documentary material and the SSPs in the following scenarios:

(1) transfer of ownership to another registered owner or change of the registered bareboat charterers, without change of Company;

(2) change of Company, without transfer of ownership to another registered owner or change of the registered bareboat charterers;

(3) transfer of flag to another Contracting Government or to a non Contracting Government, with or without change of Company; and

(4) transfer of ships from another Contracting Government or from a non Contracting Government, with or without change of Company.

12.7 Further advice will be issued, at a later stage, relating to this aspect, in particular when the documentary material or the SSP contain sensitive security related information.

13 Manning Levels[9] and Fitness for Duty

[9] Refer to paragraph B/4.28 on Manning Level.

13.1 The introduction, implementation and continuous maintenance of security measures and procedures will generate a new workload on all shipboard personnel. The degree and extent this workload will increase, is a function of the duties and responsibilities to be assigned to each member of the shipboard personnel.

13.2 Regulation V/14 of SOLAS 74 – Ship's manning has not been revised and it only requires ships to be sufficiently and efficiently manned from the point of view of safety of life at sea.

13.3 The IMO has already initiated the work for the revision of the Principles of Safe Manning contained in Resolution A.890(21) adopted by the IMO Assembly. The first stage of this work is expected to be completed through the adoption of amendments to Resolution A.890(21) during the twenty-third regular session of the Assembly of IMO which is scheduled to take place between the 24 November and 6 December, 2003.

13.4 Further work in this area, is pending and may lead to revision of regulation V/14 and possibly of regulation VIII/1- Fitness for duty of the STCW 78 as amended and of sections A-VIII/1 and B-VIII/1 of the STCW Code.

13.5 It is and remains the obligation of each Company to ensure that all shipboard personnel are fit, at all times, for duty.

13.6 The records maintained for the purpose of documenting compliance with the requirements of regulation VIII/1 of STCW 78 as amended and of section A-VIII/1 of the STCW Code shall also include and show all the hours of work, which each member of the shipboard personnel devotes, on any assigned security related duties.

13.7 Until the revision of the existing requirements relating to manning levels, Companies shall ensure that the requirements for rest, set out in section A-VIII/1 of the STCW Code, are complied with, bearing in mind all ship's security related duties.

13.8 Attention is also drawn to the fact that the provisions of the Merchant Shipping (Organisation of Working Time of Seafarers) Law, 2003 (Law 79(I) of 2003), when it will enter into force, will also apply in this respect.

14 Training and certification requirements

General

14.1 Having reached a political agreement that the measures to enhance security in the international maritime transport sector will enter into force on the 1 July 2004, it was recognised, in the early stages of the development of the measures, that although it was practically possible to adopt mandatory training and certification requirements for all persons involved with security aspects, it would have been practically impossible to train, within the limited time until the 1 July 2004, sufficient number of trainers, seafarers and other persons on security related matters without impeding the continuous functioning of the world seaborne trade.

14.2 Thus, neither the proposals relating to the adoption of amendments to the STCW 78 as amended and the STCW Code were pursued nor any other mandatory training and certification requirements were developed or adopted.

14.3 Nevertheless, it is useful to note that paragraph B/4.33 indicates that examples of possible clear grounds under regulations XI-2/9.1[10] and XI-2/9.2 may include, *among others,* when relevant:

.4 evidence or observation gained by a duly authorized officer using professional judgment that the master or the 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 *of the* 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;

14.4 Therefore, proper and prompt training of shore based and shipboard personnel is imperative. Hence, the Department strongly recommends that those concerned commence the required training as soon as possible.

Training aspects

14.5 As a result sections A/13.1 and A/13.2 only indicate that the CSO and other appropriate shore based personnel and the SSO *shall have knowledge and shall receive training*.
As far as the shipboard personnel having specific security duties and responsibilities is concerned section A/13.3 indicates that they *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*.
In the aforesaid cases the requirements of sections A/13.1, A/13.2 and A/13.3 are to be met *taking into account the guidance given in* Part B of the ISPS Code, specifically paragraphs B/13.1, B/13.2 and B/13.3.

14.6 It should be noted that sections A/13.2 and A/13.3 refer to the SSO and other shipboard personnel having specific security related duties and no specific or direct reference is made in any way to the master of the ship.

14.7 It should also be noted that Part B of the ISPS Code contains, in paragraph B/13.4, guidance in connection with all other shipboard personnel.

14.8 In connection with the reference, in section A/13.1, to other appropriate shore based personnel this personnel shall be identified by the Company and a record to this end shall be made by the CSO (or the alternate CSO).
A copy of this record does not need to be provided on board. However, this record shall be made available to the Department on request, following instructions of the Department, to RSOs issuing ISSC (or Interim ISSC) to the ships operated by the Company. In addition, this record may also need to be made available, following specific instructions of the Department, during any initial, annual, renewal or additional verifications in connection with the Document of Compliance of the Company.

14.9 Shore based personnel visiting ships shall be treated, in the SSP, when arriving on board and whilst on board as visitors, unless they have received training in accordance with, at least ,paragraph B/13.4

[10] Regulation XI-2/9 – Control and Compliance Measures.

14.10 The Department does not consider the Master of any ship as falling under the category of shipboard personnel having specific security duties and responsibilities. As a result, the Master of any ship should, at least, have full knowledge of SSO duties and responsibilities.

14.11 The following table summarises the Department's minimum recommended training requirements for the shore based personnel of the Company and of the shipboard personnel of any ship operated by the Company:

Person	Recommended Training Requirements
CSO	Section A/13.1 and paragraph B/13.1
Alternate CSO	Section A/13.1 and paragraph B/13.1
Shore based personnel assigned security related duties	Section A/13.1 and paragraph B/13.1
Other shore based personnel visiting ships	Paragraph B/13.4
Other shore based personnel not visiting ships	Paragraphs B/13.4.1 only
Master	Section A/13.2 and paragraphs B/13.1 and B/13.2
SSO	Section A/13.2 and paragraphs B/13.1 and B/13.2
Alternate SSO	Section A/13.2 and paragraphs B/13.1 and B/13.2
Shipboard personnel having specific security related duties	Section A/13.3 and paragraphs B/13.3
Other shipboard personnel	Paragraph B/13.4

14.12 In addition, the CSO, the alternate CSO, shore based personnel assigned to carry out internal audits of SSPs, should also have knowledge to carry out and document internal audits.

14.13 The Department recognises that, at the initial stages of the implementation of the special measures to enhance maritime security, it may not be possible to train all shore based and shipboard personnel to the recommended standards. However, the Department expects Companies to ensure that personnel, ashore and on board, receives adequate training to reasonably perform, at the initial stage, their assigned duties in order to avoid ships being delayed, detained or expelled from port on account of inadequate training or failure to understand or perform their assigned duties or responsibilities.
Companies are expected to understand that this approach is intended for the initial stages of implementation on the 1 July 2004 and thus it will have a very short and finite life. Therefore, Companies are expected to develop and implement plans, which ensure, at least, the adequate training of shipboard personnel, including those who may relieve person, who may be serving on board prior or after 1 July 2004.

Training methods and training establishments

14.14 It is up to each Company to decide how to train (i.e. the method of training such, as for example, classroom training at a training establishment, in house training ashore or on board, self training using selected training material or computer based or video training programmes) the CSO, the alternate CSO, and its shore-based personnel, the Master, the SSO, the alternate SSO and the shipboard personnel.

14.15 However, in this respect, the Department deams it advisable, if a Company is to use training establishments or trainers, to consider, in addition to required training skills:

(1) their expertise in relevant aspects of security;

(2) their knowledge of ship and port operations, including knowledge of ship design and construction;

(3) their knowledge of the requirements of chapter XI-2 and of the ISPS Code and relevant national and international legislation and security requirements;

(4) their knowledge of current security threats and patterns;

(5) their knowledge on recognition and detection of weapons, dangerous substances and devices;

(6) their knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

(7) their knowledge of techniques used to circumvent security measures; and

(8) their knowledge of security and surveillance equipment and systems and their operational limitations.

14.16 Furthermore, if the Company considers conducting training courses tailor-made to the Company (e.g. in-house shore or shipboard based training using external trainers), the Company concerned should also consider the following with regard to the external trainers :

(1) 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;

(2) their ability to maintain and improve the expertise of their personnel;

(3) their ability to monitor the continuing trustworthiness of their personnel; and

(4) their ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material.

14.17 The criteria set out in the preceding paragraphs also provide a guide which can be used in developing or conducting in-house shore based or shipboard training or in selecting training material (e.g. computer based training programmes or video training programmes).

14.18 The IMO is in the process of developing IMO Model Courses[11] for CSO, SSO and for Port Facility Security Officers (PFSOs). The relevant course outlines and course frameworks have been developed and agreed[12] during the 34th session of the IMO Sub-Committee on Standards of Training and Watch keeping (the STW Sub-Committee). The course outlines and course frameworks have been developed in such a way to provide, for the benefit of those concerned, the necessary information in selecting appropriate training programmes and may also be used in designing and delivering appropriate training programmes.

[11] The IMO Model Courses are expected to be published in September 2003 at the earliest.
[12] Document STW 34/WP.4 refers. A copy of this document may be obtained from the Department.

Certification of training and verification aspects

14.19 Sections A/13.1 and A/13.2 indicate that the CSO and other appropriate shore based personnel and the SSO *shall have knowledge and shall receive training*.
As far as the shipboard personnel having specific security duties and responsibilities is concerned section A/13.3 indicates that they *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*.

14.20 Sections A/13.1, A/13.2 and A/13.3 do not indicate that the person concerned (or the master of any ship) shall attend an approved training programme or shall hold a certificate or other form of documentary evidence issued by a Contracting Government.

14.21 With respect to the 1 July 2004, the Department does not, at this stage require those involved with the implementation of the required security measures and procedures, to hold documentary evidence issued by a Contracting Government attesting their training and qualifications in this respect.

14.22 The Maritime Safety Committee of IMO, at its seventy-seventh session, issued MSC/Circ. 1097, copy of which is attached, on Guidelines Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code which states:

> *"19 As an interim measure, the Committee recommended that the ISSC be accepted as prima facie evidence that training has been conducted in accordance with the ISPS Code. The flag State was responsible for deciding how that training was to be conducted, and if any additional certification was required. If a port State control inspection detected a lack of training, further action could be taken. It was anticipated that States would develop and introduce further measures after 1 July 2004, which may include the introduction of individual certificates or other documentary evidence of training."*

14.23 The intention of the Department is to require, at the stage of the initial verification (and of any subsequent verification), a verification of the fact that those involved *have the required knowledge* and *have received appropriate training*.

14.24 For the purpose of determining whether they have the *required knowledge*, the following two key questions have to be satisfactorily answered:

(1) whether, those concerned, understand their responsibilities for ship security as described in chapter XI-2 and the ISPS Code and in the ship security plan; and

(2) whether they have sufficient knowledge and ability to perform their assigned duties.

14.25 In considering the specific issue of whether they *have received appropriate training* documentary evidence of any training attended or any training carried out (including training done during the implementation process or as a result of internal audits or during drills and exercises) will be cited.

14.26 Documentary evidence indicating that a person attended a training programme will be considered on the basis of its merits. In ascertaining the merits, broadly

speaking and in addition to relevant quality and quality control criteria, the following questions will be addressed:

(1) whether the training establishment or the trainers in question meet the criteria set out in paragraphs [14.16] and [14.17] above;

(2) whether the training programme in question has been based and meets either the IMO Model Courses or the agreed course outlines and course frameworks; and

(3) the methodology used in ascertaining that the required level of knowledge has been acquired.

14.27 Documentary evidence attesting or indicating that a person has attended a training programme approved or accepted by a Contracting Government, which is also a Party to the STCW 78 as amended and is on the "White List", as meeting the requirements of chapter XI-2 and the ISPS Code (or is in accordance with the relevant IMO Model Courses or has been based on the course outlines and course frameworks agreed by the STW Sub-Committee) are very useful and provide an advantage in this process.
However, such documentary evidence will only be considered as evidence that appropriate training has been received and will not exempt those concerned from being examined on the two questions set out above during the initial (or subsequent) verification process.
In this respect, at this stage, the approach of Contracting Governments, on the issue of approving or accepting various training programmes, is uncertain.

14.28 At this stage, no advice can be offered on the attitude of Contracting Governments vis-à-vis training when they exercise control and compliance measures on the basis of the provisions of regulation XI-2/9 on Control and Compliance Measures.

15 Recognised Security Organisations

15.1 The Department is currently examining whether the various classification societies presently authorised to act on behalf of the Government of the Republic of Cyprus as recognised organisations meet, to our satisfaction, the guidance on Recognised Security Organisations (RSOs) provided in paragraph B/4.5 of the ISPS Code, in the draft EU Regulation, in the Maritime Safety Committee circular MSC/Circ. 1074, as well as certain additional requirements we consider necessary for reasons of national security.

15.2 In this respect, it is noted that we will consider for authorisation only those classification societies which are named in European Commission Decisions 96/587/EC, 98/295/EC and 98/403/EC made under the European Commission Directive 94/57EC as amended.

15.3 It is not envisaged that other organisations or legal entities will be considered for recognition and authorisation as RSOs.

15.4 It is anticipated that various conditions will be imposed in the instrument of authorisation of each RSO. These are currently under development and will include,interalia actions to be taken during the review and approval of ship security plans (e.g. in connection with the ship security assessment), during the verification process (initial, intermediate and renewal verifications) for the issue of the International Ship Security Certificate (ISSC), during the process for the issue of

Interim International Ship Security Certificate (Interim ISSC), during port State control inspections, when other States make requests for information in connection with Cyprus ships and during change of flag. These conditions will be made available for the information of ships and Companies.

16 Issue of the first International Ship Security Certificate & Failures or Suspensions of Security Measures

16.1 The Maritime Safety Committee of IMO, at its seventy-seventh session, issued MSC/Circ. 1097, copy of which is attached, on Guidelines Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code which states:

"Issue of the International Ship Security Certificate

10 The Committee concluded that a certificate should only be issued:

.1 when the ship has an approved ship security plan (SSP); and

.2 there is objective evidence to the satisfaction of the Administration that the ship is operating in accordance with the provisions of the approved plan.

11 Certificates should not be issued in cases where minor deviations from the approved plan or the requirements of SOLAS chapter XI-2 and part A of the ISPS Code exist, even if these deviations do not compromise the ship's ability to operate at security levels 1 to 3."

"Verification of Security Systems

29 In considering the question of how detailed the verification of security systems would have to be, the Committee confirmed that for all technical equipment, specified in the SSP, 100% verification was necessary, while for all operational (non-technical) security measures, a sample audit would be sufficient, to the level necessary for the auditor to verify the whole operating system."

"Subsequent failures or suspensions

12 Any subsequent failure of security equipment or systems, or suspension of a security measure that compromises the ship's ability to operate at security levels 1 to 3 have to be reported immediately, together with any proposed remedial actions, to the Administration or the RSO, if the ISSC was issued by an RSO, and the appropriate authorities responsible for any port facility which the ship is using, or the authorities of any coastal State territorial seas the ship has indicated its intention to transit and instructions requested.

13 Any failure of security equipment or systems, or suspension of a security measure that does not compromise the ship's ability to operate at security levels 1 to 3 have to be reported without delay to the Administration or the RSO, if the ISSC was issued by an RSO, and if so decided by the Administration, for their consideration with details of the equivalent alternative security measures the ship is applying until the failure or suspension is rectified together with an action plan specifying the timing of any repair or replacement.

14 The Administration or the RSO, if the ISSC was issued by an RSO, and if so decided by the Administration, may approve the alternative security measures being taken and the action plan, require amendments to such measures, require additional or alternative measures, speedier repair or replacement or take other appropriate action.

15 The International Ship Security Certificate should be withdrawn or suspended if:

.1 the alternative security measures are not, in fact, in place; or

.2 an approved action plan has not been complied with.

16 Company and Ship Security Officers and Administrations should be aware of the possible cumulative effect of individual failures or suspensions which could impair the ship's ability to operate at security levels 1 to 3."

17 Other aspects of the amendments

Automatic Identification Systems (AIS)

17.1 As a result of the amendments to regulation V/19.2.4, ships constructed before 1 July 2002 engaged on international voyages, other than passenger ships and tankers, *of 300 gross tonnage and upwards but less than 50,000 gross tonnage,* are required to fit an automatic identification system (AIS) *not later than the first safety equipment survey[13] after the 1 July 2004 or by 31 December 2004, whichever occurs earlier*.

17.2 The Department advises and strongly urges those concerned to make the necessary arrangements to obtain and fit AIS on the ships with the characteristics mentioned above as soon as possible and in any case not later than the due date.
As a result of the shortening of the period of compliance, which was previously extending up to 1 July 2007, it should be anticipated that the demand for AIS will increase considerably.

17.3 In the light of the political imperatives which dictated the specific amendment, the Department will not be able to consider applications for any "postponement".

Ship's Identification Number

17.4 The existing regulation XI/3 (which is renumbered as regulation XI-1/3) is being amended to require the permanent marking, externally and internally, of the ship's identification number[14] (commonly known as the IMO number) on *all passenger ships of 100 gross tonnage and upwards and on all cargo ships of 300 gross tonnage and upwards*.

The ship's identification number shall be permanently marked:

[13] 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.

[14] Refer to the IMO Ship Identification Number Scheme adopted by IMO with Assembly Resolution A.600(15). The ship's identification number consist of the prefix IMO followed by the seven (7) digit number allocated to each ship by Lloyd's Register of Shipping and appearing in the Register of Ships published by Lloyd's Register of Shipping. See also paragraph 28 of MSC/Circ. 1097.

(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 on 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* (the external marking)*; 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* (the internal marking).

17.5 Details on how the permanent marking shall be done, on ships constructed of steel, are provided in regulation XI-1/3.5.1 to XI-1/5.3.

17.6 Regulation XI-1/3.5.4 indicates that with respect to *ships constructed of material other than steel or metal*, the Administration shall approve the method of marking the ship identification number. The Department does not intend to issue any general guidance on the marking of the ship's identification number of ships constructed of material other than steel and will deal with this issue on a case-by-case basis. As a result, those concerned should refer the matter to the Department indicating the materials from which the ship in question is constructed and their proposals as to how to mark the ship's identification number for the Department's consideration.

17.7 *For ships constructed before 1 July 2004,* the requirements for permanent marking of the ship's identification number *shall be complied with not later than until the first scheduled dry-docking of the ship after 1 July 2004.*

For ships constructed on or after 1 July 2004 the requirements shall be complied with on the date of delivery of the ship.

17.8 For ships constructed before 1 July 2004, the Department urges those concerned to permanently mark the ship's identification number, as required by regulations XI-1/3.4 and XI-1/3.5, on the first opportunity as soon as possible and not to await *the first scheduled dry-docking of the ship after 1 July 2004.*

17.9 The Department has been using, since July 1994, as the official number of ships, aside those registered on the basis of a bareboat charter, the IMO ship's identification number.
Although it would have been reasonable to assume that the vast majority of ships, aside those registered on the basis of a bareboat charter, already comply with the internal marking requirements, it has been noted that in a number of cases, when the official number was marked on the ship, the IMO prefix was omitted.

17.10 The Department is in the process of revising and updating the guidance in connection with the Ship's Carving and Marking, required by section 8 of the Merchant Shipping (Registration of ships Sales and Mortgages) Laws, 1963 to 2000 (the Law) so as reflect the internal marking requirements.

17.11 In view of the fact that various Contracting Governments and various regional MOUs on Port State Control, will require ships calling at their ports to bear the required identification and marking, the following arrangements have to be made for the marking of ships constructed before 1 July 2004:

(1) Ships for which the Ship's Carving and Marking Note will be issued on or after 1 January 2004, either as a result of permanent registration

following a provisional one, or as a result of re-registration of a previously registered ship, or as a result of change of name or register tonnage

(2) Ships which will start flying the Cyprus flag on the basis of bareboat charter registration on or after 1 January 2004;

(3) Ships flying the Cyprus flag on the basis of a bareboat charter registration for which the period of their parallel registration will be renewed on or after 1 January 2004; and

(4) Ships flying the Cyprus flag on the basis of bareboat charter registration, other than those referred to under (2) and (3) above, which will change name on or after 1 January 2004.

Continuous Synopsis Record

17.12 A new regulation, regulation XI-1/5, is being added to the existing chapter XI (which is renumbered as chapter XI-1) requiring *every ship to which chapter I applies* to be provided with *a Continuous Synopsis Record* (CSR).

17.13 The format of the CSR is expected to be discussed and agreed at the twenty-third regular session of the Assembly of IMO which will be held between the 24 November and the 6 December 2003.

17.14 Following the agreement of the format of the CSR, the Department will initiate the preparation and issue of the CSR for each ship which will be flying the flag of the Republic of Cyprus. The Department anticipates that the CSRs will be posted at the end of March 2003. In this respect the Department urges Companies to review the details (in particular the registered address of the Company and the address from which the Company carries out safety management activities) which have been communicated to the Department and in case have occurred, which inadvertently have not been notified to the Department, to inform the Department as soon as possible.

17.15 The Department notes that with respect to ships which already fly the flag of the Republic of Cyprus, no application needs to be submitted requesting the issue of the CSR.
These will be issued by the Department otherwise and will be forwarded, unless each Company, advises the Department, to the registered address of each registered owner or registered bareboat charterer.
In case any Company wishes the CSRs for the ships it operates to be sent to them, the Company concerned should inform the Department accordingly and should indicate the names of the ships in question and their respective call signs. In such a case the Company concerned shall make the necessary arrangements for the collection of the CSRs from the Head Office of the Department.

Ship security Alert system

17.16 In accordance with Regulation XI-2 /6, all ships shall be provided with a ship security alert system as per the time schedule, indicated in the above mentioned regulation. One MSC resolution and one MSC circular have issued, Resolution 147(77), MSC/Circ:1072, copy of which are attached, on Performance Standards for a Ship Security Alert system and on Guidance on Provisions of Ship Security Alert systems.

17.17 The Department is presently considering the arrangements to be followed with respect to any ships which may hoist the flag of the Republic of Cyprus on or after the 1 July 2004.

17.18 A fee to be approved (about cy£15) in connection with the issue of the CSR will be charged on the account of each ship. [Payment of any fees or charges may be made in advance. Otherwise these have to be cleared at the time of the payment of the tonnage tax.]

Serghios S. Serghiou
Director
Department of Merchant Shipping

CC Permanent Secretary, Ministry of Communications and Works
Permanent Secretary, Ministry of Foreign Affairs
Maritime Offices of the Department of Merchant Shipping abroad
Diplomatic and Consular Missions of the Republic
Honorary Consular Officers of the Republic
Cyprus Bar Association
Cyprus Shipping Association (Sea Rovers) Ltd
Cyprus Shipping Council
Union of Cypriot Shipowners
All Recognised Classification Societies

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7735 7611
Fax: 020 7587 3210
Telex: 23588 IMOLDN G

IMO

E

Ref. T2-NAVSEC/2.11

MSC/Circ.1097
6 June 2003

GUIDANCE RELATING TO THE IMPLEMENTATION OF SOLAS CHAPTER XI-2 AND THE ISPS CODE

1 The Conference of Contracting Governments to the International Convention for the Safety of Lives at Sea (SOLAS), 1974 (London, 9 to 12 December 2002), adopted amendments to the Annex to the Convention, as amended, in particular new chapter XI-2 on Special measures to enhance maritime security; and, the new International Code for the Security of Ships and Port Facilities (ISPS Code).

2 The Maritime Safety Committee, at its seventy-seventh session (28 May to 6 June 2003), recognizing and considering the need for additional information to assist Contracting Governments and the industry with the implementation of, and compliance with new SOLAS chapter XI-2 and the ISPS Code, directed its Maritime Security Working Group to examine and provide additional guidance on specific aspects of the measures to enhance maritime security.

3 The guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code, as approved by the Committee, is given at annex.

4 Reference is also made in this context to MSC/Circ.1067 on Early implementation of measures to enhance maritime security regarding the importance of early action by all parties to ensure that the new security regime is implemented by 1 July 2004.

5 Member Governments and international organizations are invited to bring this circular to the attention of national Designated Authorities, Administrations and all parties concerned and responsible for the implementation of maritime security measures.

***

ANNEX

GUIDANCE RELATING TO THE IMPLEMENTATION OF SOLAS CHAPTER XI-2 AND THE ISPS CODE

GENERAL

1 The ensuing paragraphs are lifted from the report of the Maritime Security Working Group (MSC 77/WP.15) at MSC 77 and are considered to be of valuable guidance for the implementation of SOLAS chapter XI-2 and the ISPS Code on relevant topics.

Mobile and immobile floating units

2 Paragraphs 3.1.1.1 to .3 of part A of the ISPS Code specify the vessels and mobile offshore drilling units subject to SOLAS chapter XI-2 and ISPS Code requirements. Advice was sought on the position of floating production, storage and offloading units (FPSOs), floating storage units (FSUs) and single buoy moorings (SBMs).

3 The Committee agreed that neither of the two types of floating production, storage and offloading units (FPSOs) and floating storage units (FSUs), were ships subject to the provisions of the ISPS Code, but that they should have some security procedures in place to prevent "contamination" of ships and port facilities subject to the ISPS Code.

4 It was concluded that such units, when attached to a fixed platform, should be covered by the security regime in force for the platform.

5 Such units, when engaged in periodic short voyages between the platform and the coastal State, should not be considered to be ships engaged on international voyages.

6 The Committee also agreed that single buoy moorings (SBMs), attached to an offshore facility would be covered by that facility's security regime and if it was connected to a port facility it would be covered by the port facility security plan (PFSP).

7 In all cases the intention was to provide sufficient security to maintain the integrity of ships and port facilities covered by SOLAS and the ISPS Code.

International Ship Security Certificates (ISSC)

8 The Committee recognized that part B of the ISPS Code was albeit recommendatory, a process all parties concerned needed to go through in order to comply with part A. It was concluded that paragraph 9.4 of part A of the ISPS Code required that in order for an ISSC to be issued, the guidance in part B would need to be taken into account.

9 The Committee further specifically considered that an ISSC would not be issued unless paragraphs 8.1 to 13.8 of part B of the ISPS Code had been taken into account.

Issue of the International Ship Security Certificate

10 The Committee concluded that a Certificate should only be issued:

.1 when the ship has an approved ship security plan (SSSP); and

.2 there was objective evidence to the satisfaction of the Administration that the ship is operating in accordance with the provisions of the approved plan.

11 Certificates should not be issued in cases where minor deviations from the approved plan or the requirements of SOLAS chapter XI-2 and part A of the ISPS Code existed, even if these deviations did not compromise the ship's ability to operate at security levels 1 to 3.

Subsequent failures or suspensions

12 Any subsequent failure of security equipment or systems, or suspension of a security measure that compromises the ship's ability to operate at security levels 1 to 3 have to be reported immediately, together with any proposed remedial actions, to the Administration or the RSO, if the ISSC was issued by an RSO, and the appropriate authorities responsible for any port facility the ship is using, or the authorities of any coastal State through whose territorial seas the ship has indicated it intends to transit, and instructions requested.

13 Any failure of security equipment or systems, or suspension of a security measure that does not compromise the ship's ability to operate at security levels 1 to 3 have to be reported without delay to the Administration or the RSO, if the ISSC was issued by an RSO, and if so decided by the Administration, for their consideration with details of the equivalent alternative security measures the ship is applying until the failure or suspension is rectified together with an action plan specifying the timing of any repair or replacement.

14 The Administration or the RSO, if the ISSC was issued by an RSO, and if so decided by the Administration, may approve the alternative security measures being taken and the action plan, require amendments to such measures, require additional or alternative measures, speedier repair or replacement or take other appropriate action.

15 The International Ship Security Certificate should be withdrawn or suspended if:

.1 the alternative security measures are not, in fact, in place; or

.2 an approved action plan has not been complied with.

16 Company and Ship Security Officers and Administrations should be aware of the possible cumulative effect of individual failures or suspensions which could impair the ship's ability to operate at security levels 1 to 3.

Records

17 The Committee underlined the importance of maintaining the records required under the ISPS Code.

Training and Certification

18 Guidance on training, drills and exercises on ship security is to be found in 13.1 to13.8 of part B of the ISPS Code. The issue of evidence that Ship Security Officers and ship security personnel had, in fact, received adequate training was discussed by the Committee.

19 As an interim measure, the Committee recommended that the ISSC be accepted as *prima facie* evidence that training has been conducted in accordance with the ISPS Code. The flag State was responsible for deciding how that training was to be conducted, and if any additional certification was required. If a port State control inspection detected a lack of training, further action could be taken. It was anticipated that States would develop and introduce further measures after 1 July 2004, which may include the introduction of individual certificates or other documentary evidence of training.

Reporting requirements and communication of information

20 The Committee agreed that it was essential that the information set out in regulation 13.1.1 to 13.1.5 of SOLAS chapter XI-2 was readily available to the international shipping community.

21 Contracting Governments providing information to the Organization are, therefore, requested to confirm that they are content for the information provided under 13.1.1 to 13.1.5 to be passed by the Organization to a central source for dissemination to the worldwide shipping community.

Inspections Prior to Entering Port

22 SOLAS regulation XI-2/9.2.5 allows inspection of a ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter. Clarification was sought from the Committee on the circumstances in which an inspection could be initiated under SOLAS regulation XI-2/9.2.5.3.

23 With regard to the inspection envisaged by SOLAS regulation XI-2/9.2.5.3 the Committee, bearing in mind the requirement for "clear grounds" in regulation XI-2/9.2.4, agreed that this kind of inspection would be expected to be undertaken normally when there was information / intelligence, usually received before arrival of the ship, suggesting that there were "clear grounds" for suspecting that the ship was not in compliance with the provisions or posed a threat to the port facility.

24 Contracting Governments are considered to have the right to carry out inspections of ships, intending to enter their ports, to search for possible suspicious persons, such as terrorists, on board. The inspections would be carried out within the scope of the SOLAS Convention.

Immediate Threat

25 Clarification was also sought on the interpretation of the term "immediate threat" found in SOLAS regulation XI-2/9.3.3.

26 On the question of what was understood to be an "immediate threat" in regulation XI-2/9.3.3, the Committee agreed that this could cover two scenarios: firstly, that the ship did not comply with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code and therefore was considered to be a threat, or secondly, as in paragraph 23 above, intelligence or other information had been received indicating that the ship posed an immediate threat or was under threat itself. The Committee recognized that there may be other scenarios where, under international law, Contracting Governments could take additional measures outside of SOLAS regulation XI-2/9 for national security or defence, even if a ship fully complied with SOLAS chapter XI-2 and part A of the ISPS Code.

Responsibility for the exercise of Control Measures

27 With regard to the responsibility for control measures taken by the Contracting Governments, the Committee recognized that this might indeed differ from State to State, subject to the distribution of responsibilities to the various Government agencies of the country concerned. It was conceivable that all control measures would be undertaken by one control authority while, in other countries, traditional port State control would be conducted by PSC authorities and the security related additional control and compliance measures would be the responsibility of other designated authorities (i.e., immigration, police, navy, etc.).

Ship Identification Numbers

28 The Committee confirmed that the ship identification number (SOLAS regulation XI-1/3) to be permanently marked on the hull of the ship was the prefix "IMO" followed by the 7 digit number in accordance with resolution A.600(15).

Verification of Security Systems

29 In considering the question of how detailed the verification of security systems would have to be, the Committee confirmed that for all technical equipment, specified in the SSP, 100% verification was necessary, while for all operational (non-technical) security measures a sample audit would be sufficient, to the level necessary for the auditor to verify the whole operating system.

Voluntary nature of reporting by ships intending to enter the Territorial Sea

30 The Committee clarified that, with regard to SOLAS regulation XI-2/7, ships operating in, or intending to enter the territorial seas would report to the relevant coastal State on a voluntary basis, triggered by the ship, and that this regulation did not establish a mandatory reporting system.

Declarations of Security

31 With regard to the completion, on request of the ship, of a Declaration of Security (DoS) when interfacing with a port facility or a ship not covered by a security plan, the Committee confirmed its working assumption that, for port facilities not covered by the regulations, the coastal State would have to ensure that a contact point was to be provided ashore, with whom the ship could communicate and who would be empowered to sign the DoS while, for a ship not covered by a security plan, again there should be a designated contact point ashore (in the coastal State) or on the ship designated to sign the DoS.

_____

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7735 7611
Fax: 020 7587 3210
Telex: 23588 IMOLDN G

IMO

E

Ref. T2-NAVSEC/2.11

MSC/Circ.1072
26 June 2003

GUIDANCE ON PROVISION OF SHIP SECURITY ALERT SYSTEMS

1 The Sub-Committee on Radiocommunications and Search and Rescue (COMSAR), at its seventh session (13 to 17 January 2003), taking into account the urgency and importance of implementing SOLAS regulation XI-2/6 on Ship Security Alert Systems adopted by the Conference of Contracting Governments to the SOLAS Convention, 1974 (7-13 December 2002) to be used in the enhancement of Maritime Security, prepared the guidance on provision of ship security alert systems.

2 The Maritime Safety Committee, at its seventy-seventh session (28 May to 6 June 2003), agreed to the proposed guidance regarding Ship Security Alert Systems, as set out in the annex.

3 Member Governments are requested to bring the annexed guidance to the attention of Maritime Administrations, shipmasters, port authorities, port facility security operators, national authorities responsible for security, shipping companies, system manufacturers and designers.

***

ANNEX

GUIDANCE ON PROVISION OF THE SHIP SECURITY ALERT SYSTEM

1 Regulation 6 of SOLAS chapter XI-2 requires ships to be provided with a ship security alert system. Section A/9 of the International Ship and Port Facility Security (ISPS) Code requires ships to carry a ship security plan. Performance standards for ship security alert systems are given in resolution MSC.147(77). This Circular gives guidance on the design of ship security alert systems provided to comply with the SOLAS regulation.

2 The intent of the ship security alert system is to send a covert signal or message from a ship which will not be obvious to anyone on the ship who is not aware of the alert mechanism. It is of use therefore in circumstances where a ship wishes to inform a person ashore of a problem with a minimum number of the persons onboard aware of the action. The procedures for the security alert are agreed with the ship's Administration as part of the ship security plan and ideally should be individual to the ship. It is not intended that the ship security alert procedures should be to an internationally agreed standard or conform to any particular format for all ships.

3 Possible methods of achieving the alert are as follows:

.1 a system may employ proprietary tracking equipment provided by traffic service providers. The ship then carries a concealed equipment box working over a satellite system on its upper deck which transmits a position report at, typically, 6-hourly intervals. Interruption of power to the equipment or arming of the equipment by means of sensors or manual buttons causes the equipment to transmit a different format of position report. The tracking service providers monitor the transmission reports and inform the Company when the transmission format changes;

.2 a system may utilise modifications of GMDSS equipment.[*] Some GMDSS equipment is not very suitable for modification as it is optimised for "all station" calling and may involve manual setting of frequencies etc and provides confirmation on the ship of messages sent. In these types of systems the ship security alert contains identifiers to ensure that it is not possible to confuse it with a GMDSS distress, urgency or safety alert; and

.3 a system may utilise the exchange of messages containing key words between a ship and, typically, the Company. These messages may be by speech or data communications. Ship equipment which may be used includes cellular phones in coastal areas and satellite services away from coastal areas. It may be possible to use GMDSS VHF/MF/HF equipment in areas where there are coastal facilities for receiving addressed calls.

This list is not intended as exhaustive and is not intended to inhibit future developments.

[*] Inmarsat is developing modifications to existing equipment that will allow for this service to be implemented.

4 The ship security alert system requires two activation points, one of which should be on the bridge. These will typically be fixed or portable telephone handsets, fixed or portable keypads or fixed or portable buttons.

5 Measures should be incorporated in the activation points to avoid their inadvertent operation and the generation of false alerts.

_____

ANNEX 7

RESOLUTION MSC.147(77)
(adopted on 29 May 2003)

ADOPTION OF THE REVISED PERFORMANCE STANDARDS FOR A SHIP SECURITY ALERT SYSTEM

THE MARITIME SAFETY COMMITTEE,

RECALLING Article 28(b) of the Convention on the International Maritime Organization concerning the functions of the Committee,

RECALLING ALSO resolution A.886(21), by which the Assembly resolved that the functions of adopting performance standards for radio and navigational equipment, as well as amendments thereto, shall be performed by the Maritime Safety Committee on behalf of the Organization,

RECALLING FURTHER the provisions of the new chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, and the requirements of regulation XI-2/5, that all ships shall be provided with a ship security alert system,

RECOGNIZING that, for security reasons, a ship security alert system is necessary on board for initiating and transmitting a ship-to-shore security alert to a competent authority designated by the Administration,

HAVING CONSIDERED the recommendation on revision of resolution MSC.136(76) made by the Sub-Committee on Radiocommunications and Search and Rescue at its seventh session,

1. ADOPTS the Revised Recommendation on Performance Standards for a Ship Security Alert System, set out in the Annex to the present resolution;

2. RECOMMENDS Governments to ensure that a ship security alert system:

   (a) if installed on or after 1 July 2004, conforms to performance standards not inferior to those specified in the Annex to the present resolution;

   (b) if installed before 1 July 2004, conforms to performance standards not inferior to those specified in the Annex to resolution MSC.136(76).

ANNEX

REVISED RECOMMENDATION ON PERFORMANCE STANDARDS FOR A SHIP SECURITY ALERT SYSTEM

1 Introduction

1.1 The ship security alert system is provided to a ship for the purpose of transmitting a security alert to the shore to indicate to a competent authority that the security of the ship is under threat or has been compromised. It comprises a minimum of two activation points, one of which is on the navigation bridge. These initiate the transmission of a ship security alert. The system is intended to allow a covert activation to be made which alerts the competent authority ashore and does not raise an alarm on board ship nor alert other ships.

1.2 As required by its Administration, the competent authority receiving the alert notifies the authority responsible for maritime security within its Administration, the coastal State(s) in whose vicinity the ship is presently operating, or other Contracting Governments.

1.3 The procedures for the use of the ship security alert system and the location of the activation points are given in the ship security plan agreed by the Administration.

1.4 The ship security alert system may utilise the radio installation provided for compliance with chapter IV of the SOLAS Convention, other radio systems provided for general communications or dedicated radio systems.

2 General

2.1 In addition to complying with the general requirements set out in resolution A.694(17)[1], the ship security alert system should comply with the following performance standards.

2.2 The radio system used for the ship security alert systems should comply with relevant international standards.

3 Power supply

3.1 Where the ship security alert system is powered from the ship's main source of electrical power, it should, in addition, be possible to operate the system from an alternative source of power.

4 Activation points

4.1 Activation points should be capable of being used on the navigation bridge and in other locations. They should be protected against inadvertent operation. It should not be necessary for the user to remove seals or to break any lid or cover in order to operate any control.

[1] Publication IEC60945.

5 Operation

5.1 The activation points should operate a radio system such that transmission of the security alert does not require any adjustment of the radio system, i.e. tuning of channels, setting of modes or menu options. Operation of the activation point should not cause any alarm or indication to be raised on the ship.

5.2 The operation of the ship security alert system should not impair the functionality of the GMDSS installation.

6 Transmission of security alerts

6.1 In all cases, transmission initiated by security alert system activation points should include a unique code/identifier indicating that the alert has not been generated in accordance with GMDSS distress procedures. The transmission should include the ship identity and current position associated with a date and time. The transmission should be addressed to a shore station and should not be addressed to ship stations.

6.2 The ship security alert system, when activated, should continue the ship security alert until deactivated and/or reset.

7 Testing

7.1 The ship security alert system should be capable of being tested.

***

ANNEX 1

Who prepares the Ship Security Assessment?

Section A/8.2 states that t*he 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*.
This guidance is set out in paragraph B/8.4 which indicates that t*hose involved in a SSA should be able to draw upon expert assistance in relation to* various aspects which are listed in the aforesaid paragraph.

Section A/8.3 states that s*ubject to the provisions of section* A/*9.2.1, a recognized security organization may carry out the ship security assessment of a specific ship.*
However, it is important to note, in this respect, that section A/9.2.1 states that in case *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.*

From the point of view of the Company and the aspect of the review and approval of the SSP, section A/8.3 may be reasonably interpreted as indicating that an RSO is considered as meeting the requirements of section A/8.2 (i.e. that the RSO is considered, in the context of preparation of the SSA, as having the appropriate skills to evaluate the security of the ship) and thus a Company engaging the services of an RSO for the purpose of preparing a SSA does not need to carry out any investigations for the purpose of ascertaining this aspect.

In summary the SSA can be prepared, broadly speaking, by anyone provided it has:

(1) the appropriate[1] skills and qualifications to evaluate the security of the ship (see sections A/8.2 and A/8.3 and paragraph B/8.4) ; and
(2) the relevant information and material (see sections A/8.4 and paragraphs B/8.2 and B/8.5).

In effect the combine reading of the aforesaid provisions allows various options, which include the following:

(1) preparation of the SSA by the Company or the CSO;
(2) preparation of the SSA by the Company or the CSO and the SSO with external assistance;
(3) preparation of the SSA by a security consultant;
(4) preparation of the SSA by an RSO; or

[1] Paragraph B/4.5 also provides useful guidance in this respect.

(5) preparation of the SSA by the Administration, if the Contracting Government concerned finds necessary to do so for example due to reasons of national security.

However, if the Company engages a third part (e.g. security consultants or an RSO) section A/8.5 states that t*he ship security assessment shall be documented, reviewed, accepted and retained by the Company*.
In addition and in this respect paragraph B/8.13 provides that *if the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO*.
Furthermore, paragraph B/8.1 also indicates that w*hile 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*.
Whilst a Company may use any third party for the preparation of the SSA the combine reading of section A/8.5 and paragraph B/8.13 and section A/8.2 and paragraph B/8.1 imply that, if the Company was to adequately discharge its obligations under section A/8.5 and the CSO under section A/8.2, the Company and in particular the CSO need to have (or able to assemble) the required skills for the preparation, evaluation and acceptance of the SSA.

Section A/8 does not contain any mandatory provision relating to unauthorised access to or disclosure of the SSA (section A/9.7 specifies that t*he ship security plan shall be protected from unauthorised access or disclosure*).
However, paragraph B/8.12 indicates (although Part B o the ISPS Code has a recommendatory character) that the report of the SSA *shall be protected from unauthorized access or disclosure*.
It is prudent not only to protect the report of the SSA from unauthorised access or disclosure but also all material relating to the SSA. This aspect needs to be addressed by the Company when it engages any third party for the preparation of the SSA.

Although the SSA does not need to be approved a further aspect, which needs to be noted in connection with the SSA, is set out in section A/9.3 which states that t*he 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*.
The first step in the process of review of the SSP is to examine the SSA with a view of establishing whether it meets the requirements of section A/8.4 and paragraphs B/8.3 and B/8.6 to B/8.10 as well as any other additional national requirements. If at that stage, those reviewing the SSP, find the SSA incorrect or inadequate the submitted SSP will automatically be rejected and the Company has to start anew from the beginning.
It is reasonable to assume that the approach of those reviewing the SSA and the associated SSP will be influenced by who has prepared the SSA and not necessarily by the fact that it has been accepted by the Company or the CSO.

This aspect needs to be borne in mind by the Company when selecting the third party to prepare the SSA, as well as, when the SSA is to be prepared by the Company or the CSO with or without external assistance.

Who prepares the Ship Security Plan?

The answer to this question is similar to that for the question on who prepares the Ship Security Assessment.

Section A/9 does not state any specific mandatory requirements relating to those who may prepared the SSP and paragraph B/9 does not indicate any specific guidance in this respect.

Nevertheless, it is a prudent approach for those engaged in the preparation of the SSP to have appropriate skills.
In fact section A/9.1.1 states that s*ubject to the provisions of section* A/*9.2.1, a recognized security organization may prepare the ship security plan for a specific ship*.
This can be interpreted as providing guidance in this respect (i.e. that they should meet to the extent that is necessary the requirements of paragraph B/4.5 relating to RSOs) and a reference for assessing the skills of those involved in the preparation of the SSP.
A Company may use this reference in deciding by whom the SSP should be prepared (e.g. in setting up a team to prepare the SSP or in selecting a consultant in this respect).
In the absence of specific explicit mandatory provisions, another approach may be to consider paragraph B/8.4 (relating to ship security assessments) as providing guidance and reference in this respect.

Section A/9.1.1, as already indicated above, states that s*ubject to the provisions of section* A/*9.2.1, a recognized security organization may prepare the ship security plan for a specific ship*.
However, it is important to note that section A/9.2.1 states that in case *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*.
These aspects are also addressed and reiterated in paragraph B/9.4 which indicates that *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.*

The various options available include:

(1) preparation of the SSP by the Company or the CSO;
(2) preparation of the SSP by the Company or the CSO with external assistance;
(3) preparation of the SSP by a security consultant;
(4) preparation of the SSP by an RSO; or
(5) preparation of the SSP by the Administration, if the Contracting Government concerned finds necessary to do so for example due to reasons of national security.

Who approves the Ship Security Plan?

Section A/9.1 states that e*ach ship shall carry on board a ship security plan approved by the Administration*.

Section A/9.2 states that t*he Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations*.
However, in connection with the authorisation of RSOs to approve plans on behalf of the Administration it is important to note that section A/9.2.1 states that in case *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*.
These aspects are also addressed and reiterated in paragraph B/9.4 which indicates that *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.*

The various options are available include:

(1) approval of the SSP by Administration;
(2) approval of the SSP by an RSO acting on behalf of the Administration;
(3) approval of the SSP by another Contracting Government, if the Contracting Government concerned finds that this is acceptable and reasons of national security do not dictate otherwise.

The latter option (i.e. the approval of the SSP by another Contracting Government) is not explicitly address in the ISPS Code.
Section A/19.2.3 states that a*nother 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* and does not refer to the approval of the SSP.

It may be argued that the involvement of another Contracting Government in the verification and certification process presupposes that the SSP has been approved by the Administration.
It may also be argued that if the Administration and another Contracting Government have agreed this arrangement the approval of the SSP is valid.

It is reasonable to expect that a number of Contracting Governments, due to reasons of national security, find it undesirable to engage in the process of approval of SSPs or in the process of verification or certification of ships flying their flag other Contracting Governments.
Also, a number of Contracting Governments may, for reasons known to them, be unwilling to deal with requests in this respect.
In this context one should note the provisions of section A/9.8 and A/9.8.1 in connection with aspects of the SSP which are open for inspection during control and compliance measures under the provisions of regulation XI-2/9 (i.e. in simple terms port State control).

Who issues the International Ship Security Certificate?

In order to answer this question one has to look on the process leading to the issue of the International Ship Security Certificate (ISSC). This processes, broadly speaking, consists of three aspects, namely:

(1) the approval of the SSP;
(2) the initial verification; and
(3) the issue of the certificate.

The aspect relating to the approval of the SPP has already been discussed in the previous question.

Section A/19.2.1 states that an *International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section A/19.1.*

Section A/19.1.2 states that 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.*

Section A/19.2.2 states that the International Ship Security Certificate *shall be issued or endorsed either by the Administration or by a recognized security organization acting on behalf of the Administration.*

Section A/19.2.3 states that a*nother 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.

The companied reading of the aforesaid provisions allows various options, which include the following:

(1) an RSO approves the SSP, carries the initial verification and issues the ISSC on behalf of the Administration concerned;
(2) an RSO approves the SSP, carries the initial verification and the Administration issues the ISSC;
(3) an RSO approves the SSP, the Administration carries the initial verification and issues the ISSC;
(4) the Administration approves the SSP, carries the initial verification and issues the ISSC; and
(5) another Contracting Government approves the SSP, carries the initial verification and issues the ISSC at the request of the Administration concerned (see comments under the question who approves the plan), if reasons of national security do not dictate otherwise.

In connection with the RSO it should be noted that this need not necessarily be the classification society (in case the classification society meets the requirements of paragraph B/4.5, thus qualifies and can be recognised and authorised as an RSO) with which the ship is classed or which issues, on behalf of the Administration, the Passenger or Cargo Ship Safety Certificates.

During the process of verification of compliance with the ISM Code and the issue of the Safety Management Certificates (SMC) and Document of Compliance (DoC), a considerable number of Companies choose, as a recognised organisation (RO) for the issue of SMCs, ROs which were not the ROs which were issuing the other statutory certificates to the ships they operate.

A Company may decide, for reasons best known to them (e.g. as a result of confidentiality agreements reach with an RO in connection protection of the details contained in their safety management system or as a result of fees other service agreements) to use the RO issuing the SMC (which may not be issuing the other statutory certificates) as an RSO (provided that RO qualifies as an RSO) for the approval of the SSP, or for verifications and for the issue of the ISSC.

The ISPS Code does not prohibit any of the above. In fact it affords such flexibility. The important aspect in this process is, except where national security requirements dictate otherwise, the approval of the SSP and the initial verification for the issue of the ISSC to be carried out by the same entity.

/chc03/chc01/security/notes/note01