GUIDE FOR

SHIP SECURITY (SEC) NOTATION

MARCH 2005 (Updated January 2017 – see next page)

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA

Updates

January 2017 consolidation includes:

- March 2005 version plus Corrigenda/Editorials

Foreword

In the maritime world, safety and security are closely linked. Long before the tragic events of September 11, the mission of the American Bureau of Shipping was to promote the security of life, property, and the natural environment. For well over a century, ABS has devoted its energies to promoting safe and efficient commerce by sea through the development and application of industry consensus standards. Initially, the emphasis was on safety, and ABS applied its technology and knowledge to maintain safety through prevention of accidents caused by the forces of nature and human error. While the science of those causes is very complex and is continually being improved, they are amenable to analysis, understanding and prediction. Through the dedication and diligence of everyone in the maritime industries, the safety record of shipping has steadily improved through the years.

Maritime security introduces an additional element into the safety equation: deliberate actions by people intent on causing harm. Security has always been a concern with naval ships, and the military routinely exercise precautions to maintain the security of their ships. Commercial vessels routinely employ special security measures under certain circumstances to prevent piracy, smuggling or stowaways. Those crimes are usually economically motivated, where destruction is not the goal. Acts of terror are usually politically motivated, and ships are prime targets because of their mobility and high potential for causing extensive damage to life, property, the environment, and the transportation and economic infrastructure. The maritime community has come to the realization that ships must be made less vulnerable to security threats, both at sea and while in port.

On 12 December 2002, Contracting Governments adopted amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, to enhance the security of ships and port facilities. In addition to completing a new Chapter XI-2, "Special Measures to Enhance Maritime Security," the diplomatic conference also approved a new *International Code for the Security of Ships and of Port Facilities* (ISPS Code). Compliance with Part A of the Code is mandatory. Part B of the Code contains guidance for applying the new SOLAS requirements and Part A of the ISPS Code. The SOLAS amendments and ISPS requirements became effective on 1 July 2004. Contracting Governments may delegate some of their responsibilities under the new security regime to Recognized Security Organizations (RSO).

ABS will approve security plans, perform security audits of ships and issue International Ship Security Certificates (ISSC) on behalf of governments that have appointed ABS as an RSO for that purpose. In carrying out those responsibilities, ABS will apply the requirements of SOLAS 74, as amended and the ISPS Code, plus any additional requirements imposed by the government.

This Guide is the third revision to the Guide originally issued in January 2003. Since then, the U.S. Coast Guard has issued final rules (33 CFR Subchapter H) mandated by the Maritime Transportation Security Act of 2002. The rules require ships entering the United States to demonstrate compliance with the relevant sections of Part B of the ISPS Code (8.1–13.8). The U.S. rulemaking and consideration of similar approaches by other countries has led ABS to revise this Guide to reflect SOLAS Chapter XI-2, ISPS Code Parts A and the relevant sections of Part B (8.1 – 13.8).

ABS has prepared this *Guide for Ship Security (SEC) Notation* to assist companies and individuals in applying the security provisions of SOLAS and the ISPS Code. It is not intended to be used as a substitute for those documents. However, when used in conjunction with SOLAS, the ISPS Code, this Guide may be helpful in achieving compliance with those requirements and in obtaining the ABS **SEC** notation.

ABS offers the optional **SEC** Security Class notation to ships that comply with the international and additional requirements deemed necessary by ABS and contained in this Guide. The notation is available for all ABS classed vessels, whether or not they are required to also carry an International Ship Security Certificate (ISSC). The additional ABS requirements in the Guide are not extensive or excessive. While the notation is not required as a condition for ABS Class, ABS believes that the Security Class notation is a useful indication of the preparation and measures taken to address security concerns aboard ships.

This March 2005 edition of the Ship Security Guide is being issued to assist ABS clients in developing and implementing their ship security programs. The maritime security area is evolving rapidly, and the International Maritime Organization (IMO), the International Association of Classification Societies (IACS), governmental authorities, and ABS will all be revising their guidelines and adding to the resources available to help shipping companies meet the new requirements. . We welcome your feedback. Comments or suggestions can be sent electronically to shipsecurityguide@eagle.org.

GUIDE FOR

SHIP SECURITY (SEC) NOTATION

CONTENTS

This Page Intentionally Left Blank

SECTION 1 General

1 Scope and Application

This ABS *Guide for Ship Security* has been developed with the objective of improving security in the operation of ships. The American Bureau of Shipping recognizes the positive impact that sound security management practices have in reducing losses to the maritime industry due to terrorism, piracy, and other criminal activity. This Guide provides the maritime industry with a model for implementing ship security programs.

This Guide is intended for the use of companies operating all types of ships. The Guide's requirements are stated in general terms in order to apply to a wide variety of ships and ship operations both at sea and in port. The basic requirements that this Guide addresses have been developed by the international community for application to ships involved in international commerce and port facilities that interface with those ships. The term "ships" used in the international regulations includes passenger ships, cargo ships over 500 gross tons and mobile offshore drilling units. This Guide may also be used for other ships, such as cargo ship less than 500 gross tons and ships not involved in international commerce to improve their security programs. If requested by the ship owner, ABS will verify and certify the security program of any ship in accordance with this Guide.

The requirements of this Guide have been largely derived from the requirements prepared by the International Maritime Organization and adopted in December 2002. Those requirements consist of changes to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74), including:

- Chapter XI-2 of SOLAS, Special Measures to Enhance Maritime Security
- International Code for the Security of Ships and of Port Facilities, (ISPS Code), Part A, Mandatory Requirements
- International Code for the Security of Ships and of Port Facilities, (ISPS Code), Part B, Guidance

The ISPS Code has two Parts: Part A contains the mandatory provisions of the Code, and Part B contains additional recommendations and guidance. In June 2003, the International Maritime Organization's Maritime Safety Committee stressed that an International Ship Security Certificate should not be issued unless paragraphs 8.1 to 13.8 of part B of the ISPS Code are taken into account. Those paragraphs address the Ship Security Assessment, Ship Security Plan, Records, Company Security Officer, Ship Security Officer, and Training, Drills and Exercises. For the purpose of obtaining a **SEC** security notation from ABS, this Guide also incorporates some of the recommendations in Part B of the ISPS Code and other references on ship and port facility security that ABS believes are necessary for an effective security program. Those references are listed in Subsection 1/4 of this Guide.

Though this Guide has been developed principally to address international and United States ship security requirements, some maritime safety issues are addressed also. Security requirements cannot be allowed to place a ship and crew in an intolerable safety situation. It is necessary, as security requirements are developed and improved, that they are examined to ensure they do not violate the basic requirements for safety at sea and in port facilities associated with the ship/port interface.

This Guide is the third revision to the Guide originally issued in January 2003 and is subject to review and revision. Updates shall include, among other things, additional requirements or clarification of existing requirements. Ships certified to the requirements of this Guide shall be required to comply with the changes at the next intermediate verification that is at least a year after publication of those changes. If the change is based on changes to the international or national security requirements, the applicable compliance dates of those requirements will apply.

2 Certification

2.1 General

Companies may choose to implement security measures suitable to their organization's goals, objectives and concerns. ABS encourages all companies to consider implementation of all of this Guide's requirements as a comprehensive approach to maritime security. Ships that are classed by ABS and comply with all requirements of this Guide, and maintain full compliance, will be eligible to receive the ABS notation **SEC**. Ships that comply with all requirements of this Guide and maintain full compliance, but are not classed by ABS, will be eligible to receive ABS certification to that effect.

Where an Administration delegates authority to ABS to review, approve, and certify Ship Security Plans as a "Recognized Security Organization," (RSO), ABS will issue the certification on behalf of that government or Administration once the verification actions defined in the international regulations and supplemental national regulations are completed. ABS will advise the Company of any additional requirements, beyond those contained in this Guide, applicable to ships of a particular flag. Those additional requirements must be satisfied in order for ABS to issue documents or certifications as an RSO.

A ship that is assessed by ABS and found to meet the requirements specified in this Guide is entitled to hold a corresponding certificate. If the ship is ABS classed, it will also receive a corresponding notation in the ABS *Record*. All certificates are subject to periodic and intermediate verifications conducted for the ship. Certifications and notations are non-transferable. Assessments are based upon a sampling process. The absence of recorded nonconformities does not mean that none exist.

Nothing contained herein or in any certificate, notation or report issued in connection with a certificate or notation is intended to relieve any designer, builder, owner, manufacturer, seller, supplier, repairer, operator, insurer or other entity of any duty to inspect, or any other duty or warranty, express or implied, nor to create any interest, right, claim or benefit in any insurer or other third party.

2.2 Certification Process

Companies seeking certification to the requirements of this Guide for its ships shall fulfill the following responsibilities, some of which are more fully described in subsequent Sections of the subject Guide:

- Document, implement, and maintain a security program in accordance with the requirements of this Guide.
- Provide ABS copies of the pertinent security program, the Company Security Plan, the Ship Security Plan, and the Ship Security Assessment documentation for review and approval.
- Allow ABS access during normal working hours to ships requiring verification in order to assess the security program and determine continuing compliance with the requirements of this Guide.
- Allow ABS access during normal working hours to the offices requiring verification in order to assess the security program and determine compliance with the requirements of this Guide (suggest at annual DOC compliance audits).
- Notify ABS in a timely manner, and in writing, of port state interventions involving "security requirements" on vessels that hold security certifications or documents issued by ABS.
- Inform ABS in writing of major changes to the security program (e.g., changes in Company organizational structure that affect the security program, changes to security assessments, or changes to security plans) so that the changes may be evaluated by ABS and appropriate action taken prior to those changes being implemented.

2.3 Representations

Certification is a representation by ABS that at the time of assessment the ship had established and implemented a security program in accordance with the requirements in this Guide for the specified certificates and notations. Any noncompliant condition that has developed or manifested itself subsequent to the most recent review and certification will not be reflected in the review or certification. Certification is not a representation that the Company always acts in compliance with the security program or that the security program addresses all contingencies. Compliance with all applicable requirements remains the responsibility of the Company.

2.4 Termination

The continuance of certification or any notation is conditional upon the office and ship's continued compliance with the requirements of this Guide. ABS reserves the right to reconsider, withhold, suspend or cancel the certification or notation for noncompliance with the requirements, refusing access to a ship for an assessment or verification or nonpayment of fees which are due on account of certification and other services.

2.5 Limitation of Liability

American Bureau of Shipping shall not be liable or responsible in any respect for any inaccuracy or omission in this Guide or any other publication or document issued by ABS related to this Guide. The combined liability of American Bureau of Shipping, its officers, directors, employees, agents or subcontractors for any loss, claim, or damage arising from negligent performance or non-performance of any of its services, or from breach of any implied or express warranty of workmanlike performance in connection with those services, or from any other reason, to any person, corporation, partnership, business entity, sovereign, country or nation, will be limited to the greater of:

- $100,000, or
- An amount equal to ten times the sum actually paid for the services alleged to be deficient.

The limitation of liability may be increased up to an amount twenty-five times that sum paid for services upon receipt of the Company's written request at or before the time of performance of services and upon payment by Company of an additional fee of $10.00 for every $1,000.00 increase in the limitation.

3 Definitions

"International Ship and Port Facility Security Code" (ISPS) means the ISPS Code consisting of Part A and B as adopted by the Organization.

Company means the Owner, organization, or person who is responsible for the operation of the ship.

Declaration of Security (DoS) means an agreement reached between a ship and port facility or another ship specifying the security measures each will implement.

ISSC means International Ship Security Certificate required by SOLAS and the International Ship and Port Facility Code.

Failure means the non-fulfillment of a specified requirement or the subject matter is inappropriate for the ship which is identified at time other than at a verification for the issue of an ISSC or an Interim ISSC

Security Level means any suspicious act or circumstance threatening the security of a ship (including a mobile drilling unit and a high speed craft) or a port facility or of any ship/port interface or any ship-to-ship activity.

MARSEC means Maritime Security as used by the U.S. Coast Guard to designate security levels.

Port means the area through which ship traffic and maritime commerce flow or people are transported, including areas ashore (extending to intermodal and cargo storage areas) and on the adjacent water (to include anchorages and approaches), as defined by the designated authority.

Port Facility is a location where the ship/port interface takes place, including anchorages, berths and approaches.

Recognized Security Organization (RSO) means an organization with appropriate expertise in security and anti-terrorism matters recognized by the Administration (or the designated authority) and authorized by it to carry out assessment, verification, approval and certification activities, required by SOLAS Chapter XI-2 or by Part A of the ISPS Code, on its behalf.

Security Incident means any suspicious act or circumstance threatening the security of a ship.

Ship means any vessel (including mobile offshore drilling units, barges, small passenger vessels, etc.) that is required to have an International Ship Security Certificate or other security certificate required by a government, or that receives an **SEC** security notation from ABS or a corresponding security certificate in accordance with this Guide.

Ship/Port Interface means the interactions that occur involving movement of people, goods or provisions of port services to or from the ship.

Ship-to-Ship Activity means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

Ship Security Alert System (SSAS) means that required by SOLAS XI-2/6.

Automatic Identification System (AIS) means that required by SOLAS V19.

Continuous Synopsis Record (CSR) means that required by SOLAS XI-1/5.

Verification means an audit through a representative sample that the security system is being implemented effectively, verification that all security equipment specified in the SSP complies with applicable requirements.

4 References

The references provided in this Guide include international standards and selected government and industry guidance documents. Chapter XI-2 (Special Measures to Enhance Maritime Security) of SOLAS 74.

4.1 International and U.S. Coast Guard Security Requirements

i) SOLAS Chapter XI-2 – *Special Measures to Enhance Maritime Security* (provided in Appendix 1 to this Guide).

ii) ISPS Code Part A – Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety of Life at Sea (provided in Appendix 2 to this Guide).

iii) 33 CFR Part 104 – Vessel Security.

4.2 International and U.S. Coast Guard Guidance Documents

i) ISPS Code Part B – Recommended Guidance Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety of Life at Sea, December 2002 (provided in Appendix 3 to this Guide).

ii) Navigation and Vessel Inspection Circular titled, ‘‘Security Guidelines for Vessels’’, (NVIC 10–02), United States Coast Guard, October 2002 (provided in Appendix 8 to this Guide).

iii) Navigation and Vessel Inspection Circular titled, ‘‘Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports’’ (NVIC 9–02), United States Coast Guard, September 2002. (Copies of NVICs can be obtained from the local Coast Guard Captain of the Port or at *http://www.uscg.mil/hq/g-m/nvic.)*

iv) Navigation and Vessel Inspection Circular titled, ‘‘Security for Passenger Vessels and Passenger Terminals” (NVIC 4–02), United States Coast Guard, April 2002.

v) Navigation and Vessel Inspection Circular titled, ‘‘Security Guidelines for Facilities,’’ (NVIC 11–02), United States Coast Guard, April 2002.

vi) 33 CFR Part 101 – General Provisions

vii) 33 CFR Part 105 – Facility Security

viii) 33 CFR Part 106 – Outer Continental Shelf (OCS) Facility Security

4.3 Other Useful References

i) *Piracy and Armed Robbery Against Ships*, Marine Notice 28/2002, Australian Maritime Safety Authority, Canberra City, AU ACT 2601, December 2002.

ii) *Piracy and Armed Robbery Toward Ships*, Port Marine Circular No. 23 Of 2002, Maritime And Port Authority Of Singapore, December 2002.

iii) *Piracy And Armed Robbery Against Ships – Guidance To Shipowners And Ship Operators, Shipmasters And Crews On Preventing And Suppressing Acts Of Piracy And Armed Robbery Against Ships***,** MSC/Circ.623/Rev.3, International Maritime Organization, May 2002.

iv) *Proposed Security Manual for Ships and Mobile Offshore Drilling Units*, Republic of Liberia, MSC 75/INF 27, April 2002.

v) *AWO Model Vessel Security Plan*, The American Waterways Operators, Arlington, VA 22203, April, 2002.

vi) *Marine Safety – Tools for Risk-Based Decision Making*, ABS Consulting, Government Institutes, Rockville, MD 20850, 2002.

vii) *Guidance For Shipowners, Ship Operators And Masters On The Protection Of Ships From Terrorism And Sabotage*, International Chamber of Shipping, London, England, November 2001.

viii) *Safety and Security at Sea*, Butterworth-Heinemann, Woburn, MA 01801, 2000.

ix) *Security at Sea – Terrorism, Piracy, and Drugs*, The Nautical Institute, London, England SE1 7LQ, 1991.

x) Hawkes, K.G., *Maritime Security*, Cornell Maritime Press, 1989; Grade A Notes, 2003

SECTION 2 Maritime Security

1 General

Maritime security can only be achieved by cooperative efforts among all the parties involved in the maritime industries, with primary emphasis on ships, port facilities and governments. Although this Guide applies only to ships for the purpose of obtaining a security **SEC** notation by ABS, this Section provides additional background information that might help in understanding the international security regime. This Section gives a general overview of the ship security process and describes security levels and the roles of Governments in applying maritime security programs. Information on security requirements for port facilities is included to place the requirements for ships in perspective. It also gives an overview of the elements of basic security systems. For the purposes of this Guide, the term "ship" means any vessel that is required by a government to have a security certificate or one that complies with this Guide in order to receive an ABS **SEC** security notation.

2 Process Overview

The Company is responsible for setting the security policies for the ships it operates. As a minimum those policies must conform to international and domestic requirements, but they should also reflect the Company's objectives in maintaining safety and security onboard its vessels wherever they operate. The elements of a ship security program should include the following:

- *Company Security Officer (CSO)* – The individual in the Company who is responsible for developing and implementing the Company's security program.
- *Ship Security Assessment (SSA)* – A risk based analysis of security-related hazards or threats for each ship the Company operates. The SSA should address the particulars of the ship, its cargoes and crew, and the locations where it will operate. It should also consider the likelihood of various security-related scenarios and possible responses to those scenarios.
- *Ship Security Plan (SSP)* – A ship-specific document based on the SSA that identifies equipment, measures and procedures that are to be employed to maintain security on board the ship. The plan must address specific measures appropriate to the level of security specified by the Government or Company.
- *Ship Security Officer (SSO)* – The individual on board each ship who is responsible for ensuring that the SSP is implemented at all times while the ship is underway and in port. The SSO also is responsible for ensuring that the SSP is maintained up-to-date and that the ship's crew are trained and familiar with their security related duties. The SSO is the primary point of contact between the ship and the Port Facility Security Officer located in each port that the ship visits.
- *Documentation* – Records and certificates that confirm that the ship is in compliance with applicable security requirements. These may include records of port calls, security incidents, training and drills and certificates, such as the International Ship Security Certificate (ISSC) and ABS certification of compliance with this Guide.

There are similar and corresponding security requirements for port facilities in the ISPS Code and national regulations, to ensure that equivalent levels of security are maintained for the ship while it is in port. Those requirements are beyond the scope of this Guide. However, the CSO and SSO must maintain contact with the Port Facility Security Officer, so that all parties understand the security condition of the ship and port facility, that security is maintained while the ship is in port, and that all parties understand and are capable of taking what additional security measures are necessary if the security level changes while the ship is in port.

3 Applicability

3.1 International Requirements

Chapter XI-2 of SOLAS applies to passenger ships, cargo ships over 500 gt, high speed cargo and passenger ships and MODUs on international voyages after 1 July 2004.

3.2 ABS Requirements

ABS will review security assessments, approve security plans, conduct security audits and issue security certificates on behalf of any Administration that has authorized ABS to do so. The standards used for such statutory work will be those specified by the Administration. For information concerning authorizations and delegations to ABS by Administrations, contact your local ABS office.

Any vessel classed by ABS is eligible to apply for the ABS **SEC** notation. In order to obtain the ABS **SEC** notation, vessels must comply with all requirements contained in this Guide. It is ABS's intention that full compliance with this Guide will satisfy the requirements of SOLAS Chapter XI-2, the ISPS Code and the relevant section of Part B (8.1-13.8).

4 Security Levels

4.1 General

Chapter XI-2 of SOLAS requires that passenger ships, cargo ships over 500 gt, high speed cargo and passenger ships and MODUs on international voyages after 1 July 2004 are required to operate at a specified security level at all times. This requirement may be extended by Governments to apply to other ships flying their flags or entering their ports. Shipping companies may choose to operate their ships at a specified security level even if international or national regulations do not explicitly require them to do so. The setting of the security level applying at any particular time is normally the responsibility of Flag Administrations (for ships in general) and of Port States for port facilities and ships visiting those facilities. In general, ship and port facility security plans must address the measures to be taken at each security level. The three security levels used in the ISPS Code and in this Guide are:

- *Security Level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times;
- *Security Level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident; and
- *Security Level 3* means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

5 Administrations

Flag Administrations have a variety of security responsibilities for ships registered under their authority. These include:

- Providing guidance on the development of Ship Security Plans
- Providing guidance on measures for ships to implement at each security level
- Providing guidance on the reporting of attacks on ships
- Approving Ship Security Plans
- Issuing International Ship Security Certificates (ISSC) to ships
- Notifying ships of appropriate security levels
- Notifying other governments of ship security alerts from ships within their jurisdiction

- Specifying requirements for Declarations of Security
- Agreeing to temporary measures to be implemented if security equipment fails
- Deciding whether or not to delegate approval of Ship Security Plans, verification of ship security systems and issuing International Ship Security Certificates to Recognized Security Organizations (RSO) and overseeing such delegations

Where ABS has received authorization from an Administration to act as an RSO for ship security and the Administration has specified requirements that exceed those in this Guide, those requirements will become part of the items to be verified by ABS in the certification process performed behalf of that Administration. Those additional requirements must also be complied with in order to receive the ABS **SEC** notation.

6 Port States

Governments that have jurisdiction over port facilities are responsible for:

- Designating the port facilities in their jurisdiction which must have a port facility security officer and a port facility security plan
- Ensuring completion of a port facility security assessment for those port facilities
- Reviewing port facility security assessments and plans
- Approving the port facility security plans and relevant amendments to approved plans
- Establishing points of contact within the Government for reporting security concerns
- Setting the security levels
- Notifying affected parties of changes in security levels
- Defining when a Declaration of Security must be completed between a ship and a port facility

7 Activities not Covered by the ISPS Code

The Ship Security Plan should establish details of the procedures and security measures the ship should apply when:

.1 It is at a port of a State which is not a Contracting Government to SOLAS;

.2 It is interfacing with a ship to which the ISPS Code does not apply[1];

.3 It is interfacing with fixed or floating platforms or a mobile drilling unit on location; or

.4 It is interfacing with a port or port facility which is not required to comply with SOLAS Chapter XI-2 and Part A of the ISPS Code.

[1] Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution [3].

SECTION 3 Company Security Programs

1 Company Responsibilities

1.1 International Requirements

a. Requirements for Companies and Ships

1. Prior to entering a port and while in a port within the territory of a Contracting Government, a ship must comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship.

2. Ships must respond without undue delay to any change to a higher security level.

3. Where a ship is not in compliance with the requirements in Chapter XI-2 of SOLAS and in Part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

b. Company and Master

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

1. Who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;

2. Who is responsible for deciding the employment of the ship; and

3. In cases where the ship is employed under the terms of charter**,** who are the parties to the charter.

4. The security requirements are not intended to constrain the Master from taking or executing any decision which, in his professional judgment, is necessary to maintain the safety and security of the vessel. This includes denial of access to persons (except those duly authorized by the government) or their effects, and refusal to load cargo, including containers or other closed cargo transport units.

5. If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master may give precedence to measures intended to maintain the safety of the vessel, and take such temporary security measures as seem best under all circumstances. In such cases:

(1) The Master must, as soon as practicable, inform the relevant maritime authorities of the port and flag states;

(2) The temporary security measures must, to the highest possible degree, be commensurate with the prevailing Security Level; and

(3) The Company must ensure that such conflicts are resolved to the satisfaction of the relevant maritime authorities of the port and flag states, and that the possibility of recurrence is minimized

6. The Ship Security Plan must contain a clear statement emphasizing the Master's authority. The Company shall establish in the Ship Security Plan that the Master has the overriding authority and responsibility to make decisions with respect to the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

7. The Company must ensure that the Company Security Officer, the Master and the Ship Security Officer are given the necessary support to fulfill their duties and responsibilities in accordance with Chapter XI-2 of SOLAS and Part A of the ISPS Code.

c. Company Security Officer

1. The Company must designate a Company Security Officer. A person designated as the Company Security Officer may act as the Company Security Officer for one or more ships, depending on the number or types of ships the Company operates, provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate, designate several persons as Company Security Officers, provided it is clearly identified for which ships each person is responsible.

2. In addition to those specified elsewhere in the Guide, the duties and responsibilities of the Company Security Officer include, but are not limited to:

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

3. Qualifications.

(1) The CSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security administration and organization of the Company's vessels;

(ii) Vessel, facility, and port operations relevant to that industry;

(iii) Vessel and facility security measures, including the meaning and the consequential requirements of the different Security Levels;

(iv) Emergency preparedness and response and contingency planning;

(v) Security equipment and systems and their operational limitations;

(vi) Methods of conducting audits, inspection and control and monitoring techniques; and

(vii) Techniques for security training and education, including security measures and procedures.

(2) In addition to knowledge and training above, the CSO must have general knowledge through training or equivalent job experience in the following, as appropriate:

(i) Relevant international conventions, codes, and recommendations;

(ii) Relevant government legislation and regulations;

(iii) Responsibilities and functions of other security organizations;

(iv) Methodology of Vessel Security Assessment;

(v) Methods of vessel security surveys and inspections;

(vi) Instruction techniques for security training and education, including security measures and procedures;

(vii) Handling sensitive security information and security-related communications;

(viii) Knowledge of current security threats and patterns;

(ix) Recognition and detection of dangerous substances and devices;

(x) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(xi) Techniques used to circumvent security measures;

(xii) Methods of physical screening and non-intrusive inspections;

(xiii) Security drills and exercises, including drills and exercises with facilities; and

(xiv) Assessment of security drills and exercises.

(xv) Ship and port operations

(xvi) Ship and port facility security measures

(xvii) Methods of physical searches and non-intrusive inspections

4. In addition to those responsibilities and duties specified elsewhere, the CSO must, for each vessel for which he or she has been designated:

(1) Keep the vessel apprised of potential threats or other information relevant to its security;

(2) Ensure a Ship Security Assessment (SSA) is carried out;

(3) Ensure a Ship Security Plan (SSP) is developed, approved, and maintained;

(4) Ensure the SSP is modified when necessary;

(5) Ensure vessel security activities are audited;

(6) Arrange for required governmental inspections;

(7) Ensure the timely or prompt correction of problems identified by audits or inspections;

(8) Enhance security awareness and vigilance within the organization;

(9) Ensure personnel receive adequate security training;

(10) Ensure communication and cooperation between the vessel and the port and facilities with which the vessel interfaces;

(11) Ensure consistency between security requirements and safety requirements;

(12) Ensure that when sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately;

(13) Ensure compliance with an Alternative Security Program as authorized by the government or approved equivalents, as appropriate; and

(14) Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

1.2 Company and Port State Requirements

(a) The Company must be knowledgeable of governmental regulations to ensure that the vessel operates in compliance with the security requirements of the flag Administration, the Port State, and as appropriate, the Coastal State..

(b) For each vessel, the Company must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Ensure security records are kept;

(3) Ensure that adequate coordination of security issues takes place between ships and facilities, including the execution of a Declaration of Security (DoS);

(4) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival;

(5) Ensure security communication is readily available;

(6) Ensure coordination with and implementation of changes in Security Level;

(7) Ensure that security systems and equipment are installed and maintained;

(8) Ensure that all access to and from the ship, including the embarkation of persons and their effects, is controlled;

(9) Ensure that restricted areas are controlled;

(10) Ensure that cargo and vessel stores and bunkers are handled in compliance with security requirements;

(11) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

(12) Provide the Master, or for vessels on U.S. domestic routes only, the CSO, with the following information:

(i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractors, concessionaires (for example, retail sales outlets, casinos, etc.);

(ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and

(iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and

(13) Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

1.3 Company Security Plan

1.3.1 Company Security Plan

For any company that wishes to obtain certification by ABS of its security program for specific ships, there shall be a Company Security Plan that documents the following items:

- The company security policy
- The company personnel responsible for managing the security program and their access to management
- The authority of ship Masters to ensure safety of the crew, passengers, and the ship, regardless of security issues
- The duties of the Company Security Officer
- The company audit program that addresses security issues
- A record of all security incidents involving Company ships

A copy of the Company Security Plan shall be submitted to ABS for approval to allow ABS to verify compliance with this Guide. It should be accompanied by a current security audit report for company security activities (ship audits will be reviewed at the time of the Ship Security Plan review).

1.3.2 Delegation of Authority

The Company Security Plan shall state that the Company Security Officer has the authority to report directly to the highest level of company management for matters of security.

1.3.3 Dual Responsibilities

If a company assigns the Company Security Officer responsibility to a person that serves on a specific ship (e.g., a Ship Security Officer), the Company Security Plan shall specify how that person will be able to meet all of the requirements for the Company Security Officer (e.g., requirements for ensuring communication and coordination between Ship Security Officers and port facility security officers, providing corporate oversight of ship security functions).

1.3.4 Maritime Intelligence Awareness Program

The Company Security Plan shall also include a requirement for the Company Security Officer to maintain awareness of security threat information (e.g., intelligence reports, reports of suspicious activities, acts of piracy, criminal activity) for the areas in which the company's ships operate. That information should be used in performing ship security assessments and should be periodically provided to the Company's Ship Security Officers for their use in security planning and implementation.

SECTION 4 Ship Security Programs

1 Ship Security Officer

1.1 International Requirements

a. General

1. A SSO may perform other duties within the Company's organization, provided he or she is able to perform the duties and responsibilities required of the SSO for each such vessel.

2. For manned vessels, the SSO must be a member of the crew.

3. For unmanned vessels, the same person may serve as the Vessel Security Officer for more one than one unmanned vessel. If a person serves as the Vessel Security Officer for more than one unmanned vessel, the name of each unmanned vessel for which he or she is the Vessel Security Officer must be listed in the Vessel Security Plan.

4. The Vessel Security Officer of any unmanned barge and the SSO of any towing vessel interfacing with the barge must coordinate and ensure the implementation of security measures applicable to both vessels during the period of their interface.

5. The Vessel Security Officer may assign security duties to other vessel personnel; however, the Vessel Security Officer remains responsible for these duties

b. Ship Security Officer

1. A Ship Security Officer must be designated on each ship and must be identified in the Ship Security Plan.

2. The Ship Security Officer must have knowledge and have received training in all aspects of security involving the ship.

3. Qualifications

   The SSO must have general knowledge, through training or equivalent job experience, in the following:

   (1) Those items listed for the Company Security Officer;

   (2) Vessel layout;

   (3) The Ship Security Plan (SSP) and related procedures, including scenario- based response training;

   (4) Crowd management and control techniques;

   (5) Operations of security equipment and systems; and

   (6) Testing and calibration of security equipment and systems, and their maintenance while at sea.

4. The duties and responsibilities of the Ship Security Officer include, but are not limited to:

   - undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
   - maintaining and supervising the implementation of the Ship Security Plan, including any amendments to the plan;

- coordinating the security aspects of handling cargo and ship's stores with other shipboard personnel and with port facility security officers;
- proposing modifications to the Ship Security Plan;
- reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
- enhancing security awareness and vigilance on board;
- ensuring that adequate security training has been provided to shipboard personnel;
- reporting all security incidents to the Company Security Officer;
- coordinating implementation of the Ship Security Plan with the Company Security Officer and the port facility security officer;
- ensuring that security equipment is properly operated, tested, calibrated and maintained, if any, and.
- ensuring consistency between security requirements and the proper treatment of vessel personnel affected by those requirements
- completing the Declaration of Security on behalf of the ship.

c. Vessel Personnel with Security Duties

General

Company and vessel personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current security threats and patterns;

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Techniques used to circumvent security measures;

(e) Crowd management and control techniques;

(f) Security-related communications;

(g) Knowledge of emergency procedures and contingency plans;

(h) Operation of security equipment and systems;

(i) Testing and calibration of security equipment and systems, and their maintenance while at sea;

(j) Inspection, control, and monitoring techniques;

(k) Relevant provisions of the Ship Security Plan;

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different Security Levels.

d. Other Shipboard Personnel

General

All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:

.1 the meaning and the consequential requirements of the different security levels;

.2 knowledge of the emergency procedures and contingency plans;

.3 recognition and detection of weapons, dangerous substances and devices;

.4 recognition, on a nondiscriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security; and

.5 techniques used to circumvent security measures

2 Ship Security Alert System

2.1 International Requirements

a. Ship Security Alert System

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

   - ships constructed on or after 1 July 2004;
   - passenger ships**,** including high-speed passenger craft**,** constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;
   - oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft**,** of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004; and
   - other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.
   - must be included in the ship security plan

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

   - initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration**,** which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;
   - not send the ship security alert to any other ships;
   - not raise any alarm on-board the ship; and
   - continue the ship security alert until deactivated and/or reset.

3. The ship security alert system shall:

   - be capable of being activated from the navigation bridge and in at least one other location; and
   - conform to performance standards not inferior to those adopted by the Organization.

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

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

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

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

3 Ship Security Assessments

3.1 General

a. Ship Security Assessment

1. The Ship Security Assessment is an essential and integral part of the process of developing and updating the Ship Security Plan.

2. The Company Security Officer shall ensure that the Ship Security Assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with the ISPS Code.

3. Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs.

   Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment.

   The CSO should follow any specific guidance offered by the Contracting Governments.

4. Security assessments should be performed based on examination of specific threat scenarios, with consideration of the vulnerability of the ship and the consequence of those scenarios.

5. The Ship Security Assessment shall be documented, verified and retained by the Company

3.2 On-scene Security Survey

1. The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

   .1 ensuring the performance of all ship security duties;

   .2 monitoring restricted areas to ensure that only authorized persons have access;

   .3 controlling access to the ship, including any identification systems;

   .4 monitoring of deck areas and areas surrounding the ship;

   .5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);

   .6 supervising the handling of cargo and the delivery of ship's stores; and

   .7 ensuring that ship security communication, information, and equipment are readily available.

   .8 identification of existing security measures, procedures and operations;

   .9 identification and evaluation of key shipboard operations that it is important to protect;

   .10 identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and

   .11 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

3.3 Ship Security Assessment Requirements

(a) The Vessel (Ship) Security Assessment (SSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single SSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the SSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a SSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel and vessel-to-facility interface practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

(e) The following background information must be provided to any person who conducts the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) The locations where the ship's stores and essential maintenance equipment is stored;

(vii) Changes in the tide which may have an impact on the vulnerability or security of the ship

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous SSA, if any;

(4) Emergency and stand-by equipment available to maintain essential services;

(5) Number of ship personnel and any existing security duties to which they are assigned;

(6) Training requirements and practices for personnel on board the vessel;

(7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and ship's personnel;

(8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;

(9) Existing agreements with private security companies providing waterside or vessel security services; and

(10) Existing security measures and procedures, including:

(i) Inspection and control procedures;

(ii) Identification systems;

(iii) Surveillance and monitoring equipment;

(iv) Personnel identification documents;

(v) Communication systems;

(vi) Alarms;

(vii) Lighting;

(viii) Access control systems; and

(ix) Other security systems.

(f) An on-scene survey of each vessel must be conducted. The on-scene survey is to verify or collect required information. It consists of an actual survey that examines and evaluates protective measures, procedures, and operations. (See 4/3.2)

(g) In conducting the SSA, the Company Security Officer must analyze the vessel background information and the on-scene survey, and provide recommendations for the security measures the vessel should include in the Ship Security Plan (SSP). This includes but is not limited to the following:

(1) Restricted areas;

(2) Response procedures for fire or other emergency conditions;

(3) Security supervision of ship personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;

(4) Frequency and effectiveness of security patrols;

(5) Access control systems, including identification systems;

(6) Security communication systems and procedures;

(7) Security doors, barriers, and lighting;

(8) Any security and surveillance equipment and systems;

(9) Possible security threats, including but not limited to:

(i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;

(ii) Hijacking or seizure of the vessel or of persons on board;

(iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;

(iv) Unauthorized access or use, including presence of stowaways;

(v) Smuggling dangerous substances and devices;

(vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;

(vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;

(viii) Attacks from any side while at berth or at anchor; and

(ix) Attacks while at sea; and

(10) Evaluating the potential of each identified point of access, including open weather decks, that might be used to breach security.

(h) SSA report.

(1) A written SSA report must be included as part of the SSP. The SSA report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) Existing security measures, procedures, and operations;

(iii) A description of each vulnerability found during the assessment;

(iv) A description of security countermeasures that could be used to address each vulnerability;

(v) A list of the key vessel operations that are important to protect;

(vi) The likelihood of possible threats to key vessel operations; and

(vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.

(2) The SSA report must address the following elements on board or within the vessel:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility.

(3) The SSA must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Vessel personnel;

(ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;

(iii) Capacity to maintain safe navigation and emergency response;

(iv) Cargo, particularly dangerous goods or hazardous substances;

(v) Vessel stores;

(vi) Any vessel security communication and surveillance systems; and

(vii) Any other vessel security systems, if any.

(4) The SSA must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on vessel personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The SSA must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the vessel, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Supervising the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the vessel; and

(vii) The ready availability of security communications, information, and equipment.

(6) The SSA must be documented and the SSA report retained by the Company with the SSP. The SSA and SSP must be protected from unauthorized access or disclosure.

(i) The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

(j) Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

(k) If the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO.

4 Ship Security Plans

4.1 General

1. The Company Security Officer (CSO) has the responsibility of ensuring that a Ship Security Plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

2. All SSPs should:

.1 detail the organizational structure of security for the ship;

.2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

.3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;

.4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;

.5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;

.6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

.7 reporting procedures to the appropriate Contracting Governments contact points.

3. Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

4. All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognized Security Organisation (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.

5. CSOs and Ship Security Officers (SSOs) should develop procedures to:

   .1 assess the continuing effectiveness of the SSP; and

   .2 prepare amendments of the plan subsequent to its approval.

6. The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and Part A of this Code will be carried out. Otherwise, the process of issue to the ship of the required International Ship Security Certificate cannot be carried out.

   If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by, the Administration.

4.2 Ship Security Plan Requirements

1. Each ship must carry on board a Ship Security Plan approved by the Administration. The plan shall make provisions for the three security levels as defined in the ISPS Code.

2. The Administration may entrust the review and approval of Ship Security Plans, or of amendments to a previously approved plan, to a recognized security organization, provided the RSO has not been involved in either the preparation of the Ship Security Assessment or of the Ship Security Plan, or of the amendments, under review.

3. Submission of Ship Security Plans, or a plan amendment, for approval shall be accompanied by the Ship Security Assessment on which the plan or amendment was based.

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

   - measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized from being taken on board the ship;
   - identification of restricted areas and measures for the prevention of unauthorized access to the ship and to restricted areas on board;
   - procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
   - procedures for responding to any security instructions Contracting Governments may give at security level 3;
   - procedures for evacuation in case of security threats or breaches of security;
   - security related duties assigned to shipboard personnel;
   - procedures for auditing the security activities;
   - procedures for training, drills and exercises associated with the plan;
   - procedures for interfacing with port facility security activities;
   - procedures for the periodic review of the plan and for updating;
   - procedures for reporting security incidents;
   - identification of the Ship Security Officer;
   - identification of the Company Security Officer including 24-hour contact details;

- procedures and schedule for inspection, testing, calibration, and maintenance of any security equipment on board
- identification of the locations where the ship security alert system activation points are fitted
- procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting, and to limit false alerts

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

6. The Administration shall determine which changes to an approved Ship Security Plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in Chapter XI-2 of SOLAS and Part A of the ISPS Code. The nature of the changes to the Ship Security Plan or the security equipment that have been specifically approved by the Administration shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

7. The plan may be kept in an electronic format. In such a case, it shall be protected by means to prevent it from being deleted, destroyed or overwritten.

8. The plan must be protected from unauthorized access or disclosure.

9. Ship Security Plans are not generally subject to inspection by officers of a port state. However, if there are clear grounds for believing that the ship is in violation of the requirements of Chapter XI-2 of SOLAS or of the ISPS Code, limited access to the specific sections of the plan relating to the non-compliance is allowed, but only with the consent of the Flag Administration or the Master of the ship.

10. Must address each vulnerability identified in the Ship Security Assessment.

11. Must describe security measures for each security level.

12. Must have the statement regarding the Master's authority

13. May cover more than one vessel to the extent that they share similarities in physical characteristics and operations.

4.3 Organization and Performance of Ship Security Duties

(a) The Ship Security Plan should delineate the following relative to the different security levels:

.1 The duties and responsibilities of all shipboard personnel with a security role;

.2 The procedures or safeguards necessary to maintain continuous communications at all times;

.3 The procedures needed to assess the continuing effectiveness of security procedures and security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;

.4 The procedures and practices to protect security-sensitive information held in paper or electronic format;

.5 The type and maintenance requirements, of security and surveillance equipment and systems, if any;

.6 The procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and

.7 Procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

5 Training and Drills

5.1 General

a. Training and Drills

1. The Company Security Officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in Part B of the ISPS Code.

2. The Ship Security Officer shall have knowledge and have received training, taking into account the guidance given in Part B of the ISPS Code

3. Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the Ship Security Plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part B of the ISPS Code.

4. To ensure the effective implementation of the Ship Security Plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in the ISPS Code.

5.2 Training Requirements

Security Training for All Vessel Personnel

All vessel personnel, including contractors, whether part-time, fulltime, temporary, or permanent, must have knowledge of, through training or equivalent job experience, the following:

(a) Relevant provisions of the Ship Security Plan;

(b) The meaning and the consequential requirements of the different Security Levels, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

Drill and exercise requirements.

(a) General – Drills and exercises must test the proficiency of vessel personnel in assigned security duties at all Security Levels and the effective implementation of the Ship Security Plan (SSP). They must enable the Ship Security Officer (SSO) to identify any related security deficiencies that need to be addressed.

(b) Drills.

(1) The SSO must ensure that at least one security drill is conducted at least every 3 months, except when a vessel is out of service due to repairs or seasonal suspension of operation, provided that in such cases a drill must be conducted within one week of the vessel's reactivation. Security drills may be held in conjunction with non-security drills where appropriate.

(2) Drills must test individual elements of the SSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility's scheduled drill.

(4) Drills must be conducted within one week whenever the percentage of vessel personnel with no prior participation in a vessel security drill on that vessel exceeds 25 percent.

(c) Exercises.

(1) Various types of exercises which may include participation of Company Security Officers, port facility security officers, relevant authorities of Contracting Governments as well as Ship Security Officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability, and response.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the above.

(3) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include the substantial and active participation of relevant company and vessel security personnel, and may include facility security personnel and government authorities depending on the scope and the nature of the exercises.

(6) Company participation in an exercise with another Contracting Government should be recognized by the Administration.

Drills and Training for Rest of ship's Crew

(a) In addition to specific training for personnel that are involved in implementing security actions, all of the ship's crew should receive security awareness training as part of their general orientation and training activities. This awareness training should address issues such as:

- limiting discussion about specifics of the ship (e.g., cargo, routes, equipment, crew size) with non-company personnel to those personnel that need to know in order to service the ship
- reporting suspicious acts or behavior related to the ship both on/near the ship and when personnel are on shore leave
- protection of company-supplied identification cards or other documentation

A high level of awareness by company personnel of these simple measures can help prevent the ship from becoming an easy target.

6 Ship Security Records

6.1 General

a. Records

1. Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of the Ship Security Plans are being implemented.

2. Records may be kept in any format but should be protect from unauthorized access or disclosure

b. ISPS Code Part A, Section 10 – Records

1. Records of the following activities addressed in the Ship Security Plan must be kept on board for at least the time frame covering the previous 10 ports of call.

- training, drills and exercises;
- security threats and security incidents;
- breaches of security;
- changes in security level;
- communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- internal audits and reviews of security activities;
- periodic review of the Ship Security Assessment;
- periodic review of the Ship Security Plan;
- implementation of any amendments to the plan; and
- maintenance, calibration and testing of security equipment, if any including testing of the ship security alert system.

2. The records may be kept in an electronic format. In such a case, they shall be safeguarded by procedures to prevent their unauthorized deletion, destruction or amendment.

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

6.2 Records Requirements

Vessel record-keeping requirements.

(a) Unless otherwise specified, the Ship Security Officer must keep required records for at least 2 years and make them available to the government authorities upon request.

(b) Records may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) Training. For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) Drills and exercises. For each drill or exercise, the date held, description of drill or exercise, list of participants; and any best practices or lessons learned which may improve the Ship Security Plan (SSP);

(3) Incidents and breaches of security. Date and time of occurrence, location within the port, location within the vessel, description of incident or breaches, to whom it was reported, and description of the response;

(4) Changes in Security Levels. Date and time of notification received, and time of compliance with additional requirements;

(5) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, the date and time, and the specific security equipment involved;

(6) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

(7) Declaration of Security (DoS). Manned vessels must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) Annual internal audits of the SSP. For each annual audit, a letter certified by the SSO stating the date the audit was completed.

(9) Annual periodic reviews of the SSA and the SSP maintained.

(c) Required security records must be protected from unauthorized access or disclosure.

(d) Records must be kept in the working language or languages of the ship or translation in either English, French or Spanish.

(e) Security-related records required under the international requirements and any additional records specified by ABS shall be kept for 5 years to allow internal audit review and to provide evidence of program compliance for periodic verification by ABS

6.3 Company and Vessel Records

(a) The Company shall ensure that the Master has available on board, updated documented information through which officers duly authorized by a Contracting Government can determine:

- who appoints the members of the crew or other persons employed or engaged on board the ship in any capacity
- who decided and decides the employment of the ship; and
- in cases where the ship is employed under the terms of charter party, who signed the charter party on behalf of the owner of the ship

(b) Ships must be able to provide the following information:

- that the ship possesses a valid Certificate and the name of its issuing authority;
- the security level at which the ship is currently operating;
- the security level at which the ship operated in the 10 previous port calls;
- any special or additional security measures that were taken by the ship in the 10 previous port calls;
- that the appropriate ship security procedures were maintained during any ship-to-ship activity within the timeframe of the previous 10 port calls; or
- other practical, security-related information, but not details of the Ship Security Plan

7 Audits and Reviews

7.1 General

(a) Internal audits and reviews of the Ship Security Plan and its effective implementation shall be carried out annually onboard each ship in the Company's fleet. Records of any nonconformance and corrective action associated with the internal audit or review shall be identified within an internal audit report. A copy of this internal audit report shall be maintained on board the ship for review for external verification by either the RSO or the Administration.

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

(c) The company security audit program shall be described in the Company Security Plan, including responsibility for resolving audit findings and reporting the status of open security audit findings to corporate management. A periodic report of the status of audit findings shall be available on the ship for findings related to that ship and at the location of the Company Security Officer for all ships for which that officer has security responsibility

7.2 Audit and Review Requirements

(1) The CSO or SSO must ensure an audit and review of the SSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the SSP certifying that the SSP meets the applicable security requirements.

(2) The SSP must be audited if there is a change in the company's or vessel's ownership or operator, or if there have been modifications to the vessel, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the SSP as a result of modifications to the vessel may be limited to those sections of the SSP affected by the vessel modifications.

(4) Unless impracticable due to the size and nature of the company or the vessel, personnel conducting internal audits of the security measures specified in the SSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit or review require amendment of either the SSA or SSP, the SSO or CSO must submit the amendments to the approving authority for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended SSP meets the applicable requirements.

8 Declaration of Security

8.1 General

a. Declaration of Security

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

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

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

Requests for the completion of a Declaration of Security must be acknowledged by the applicable port facility or ship.

The Declaration of Security is completed by:

- the Master or the Ship Security Officer on behalf of the ship; and, if appropriate,
- the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

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

A copy of the Declaration of Security must be kept by both the ship and the port facility.

The Declaration of Security shall be made available to government authorities upon request.

Copies of Declarations of Security must be kept for at least the last 10 port calls.

b. The SSP should detail how requests for DoS from a port facility will be handled and the circumstances under which the ship itself should request a DoS.

8.2 Declaration of Security Requirements

(a) Procedures must be established for requesting a DoS and for handling DoS requests from a facility or other vessel.

(b) At Security Level 1, the Master or Ship Security Officer (SSO), or their designated representative, of any cruise ship or manned vessel carrying Certain Dangerous Cargoes in bulk may, or at the direction of the Contracting Government, complete and sign a DoS with the SSO or Facility Security Officer or their designated representative, of any vessel or facility with which it interfaces.

(1) For a vessel-to-facility interface, prior to arrival of a vessel to a facility, the Facility Security Officer and Master, SSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon a vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the Facility Security Officer or Master, SSO, or designated representatives must sign the written DoS.

(2) For a vessel engaging in a vessel-to-vessel interface, prior to the interface, the respective Masters, SSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon the vessel-to-vessel interface and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, SSOs, or designated representatives must sign the written DoS.

(c) At Security Levels 2 and 3, the Master, SSO, or designated representative must sign and implement a DoS prior to any vessel-to-vessel interface.

(d) At Security Levels 2 and 3, the Master, SSO, or designated representative must sign and implement a DoS with the Facility Security Officer of any facility on which it calls prior to any cargo transfer operation or passenger embarkation or disembarkation.

(e) When the Security Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented.

(f) The government may require at any time, at any Security Level, any manned vessel to implement a DoS with the SSO or Facility Security Officer prior to any vessel-to-vessel or vessel-to-facility interface when he or she deems it necessary.

8.3 ISPS Code Part B Guidance, Paragraph 9.52 – Declarations of Security

8.4 Additional ABS Requirements

No additional requirements.

8.5 Additional ABS Guidance

No additional guidance provided.

9 Verification and Certification of Ships

9.1 International Requirements

a. SOLAS Chapter XI-2

No specific requirements.

b. ISPS Code Part A

Section 11 – Company Security Officer

The Company Security Officer arranges for the initial and subsequent verifications of the ship by the Administration or the recognized security organization

The Company Security Officer ensures that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with.

Section 12 – Ship Security Officer

The Ship Security Officer reports to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions.

Section 19 – Verification and Certification for Ships

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

- *an initial verification* before the ship is put in service or before the required certificate is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of SOLAS Chapter XI-2, the ISPS Code, and the approved Ship Security Plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of SOLAS Chapter XI-2 and the ISPS Code, is in satisfactory condition and fit for the service for which the ship is intended;
- *a renewal verification* at intervals specified by the Administration, but not exceeding five years. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of SOLAS Chapter XI-2, the ISPS Code; and the approved Ship Security Plan; and is in satisfactory condition and fit for the service for which the ship is intended;
- *at least one intermediate verification.* The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;
- *any additional verifications* as determined by the Administration.
- *The Company Security Plan, amendments and audit findings,* are to be reviewed at intermediate, renewal and, where necessary, additional shipboard verifications.

The verifications of ships must be carried out by officers of the Administration or a recognized security organization authorized by the Administration.

The Administration will fully guarantee the completeness and efficiency of the verification and will undertake to ensure the necessary arrangements to satisfy this obligation.

The security system and any associated security equipment of the ship after verification must be maintained to conform with SOLAS Chapter XI-2, the ISPS Code and the approved Ship Security Plan. After any verification has been completed, no changes may be made to the security system, any associated security equipment or the approved Ship Security Plan without the sanction of the Administration.

Issue or Endorsement of Certificate

An International Ship Security Certificate (ISSC) may be issued after the initial or renewal verification.

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

Another Contracting Government may, at the request of the Administration, cause the ship to be verified and, if satisfied that the requirements are complied with, may 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 the ISPS Code.

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

A certificate so issued will contain a statement to the effect that it has been issued at the request of the Administration and it will have the same force and receive the same recognition as the certificate issued by the Administration.

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

Duration and Validity of Certificate

An International Ship Security Certificate issued under this Guide shall be issued for a period which shall not exceed five years.

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

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

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

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

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

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

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

APPENDIX 1 SOLAS Chapter XI-2 – Special Measures to Enhance Maritime Security

CHAPTER XI-2
SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

Regulation 1
Definitions

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

.1 *Bulk carrier* means a bulk carrier as defined in regulation IX/1.6.

.2 *Chemical tanker* means a chemical tanker as defined in regulation VII/8.2.

.3 *Gas carrier* means a gas carrier as defined in regulation VII/11.2.

.4 *High-speed craft* means a craft as defined in regulation X/1.2.

.5 *Mobile offshore drilling unit* means a mechanically propelled mobile offshore drilling unit, as defined in regulation IX/1, not on location.

.6 *Oil tanker* means an oil tanker as defined in regulation II-1/2.12.

.7 *Company* means a Company as defined in regulation IX/1.

.8 *Ship/port interface* means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship.

.9 *Port facility* is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.

.10 *Ship to ship activity* means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

.11 *Designated Authority* means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.

.12 *International Ship and Port Facility Security (ISPS) Code* means the International Code for the Security of Ships and of Port Facilities consisting of Part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization, provided that:

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

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

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

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

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

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

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

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

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

Regulation 2
Application

1 This chapter applies to:

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

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

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

.1.3 mobile offshore drilling units; and

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

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

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

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

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

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

Regulation 3
Obligations of Contracting Governments with respect to security

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

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

Regulation 4
Requirements for Companies and ships

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

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

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

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

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

Regulation 5
Specific responsibility of Companies

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

.1 who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;

.2 who is responsible for deciding the employment of the ship; and

.3 in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

Regulation 6
Ship security alert system

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

.1 ships constructed on or after 1 July 2004;

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

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

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

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

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

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

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

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

3 The ship security alert system shall:

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

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

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

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

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

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

Regulation 7

Threats to ships

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

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

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

.1 the current security level;

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

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

Regulation 8
Master's discretion for ship safety and security

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

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

Regulation 9
Control and compliance measures

1 Control of ships in port

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

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

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

2 Ships intending to enter a port of another Contracting Government

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

.1 that the ship possesses a valid Certificate and the name of its issuing authority;

.2 the security level at which the ship is currently operating;

.3 the security level at which the ship operated in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.5 that the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified in paragraph 2.3; or

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

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

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

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

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

2.5 Such steps are as follows:

.1 a requirement for the rectification of the non-compliance;

.2 a requirement that the ship proceed to a location specified in the territorial sea or internal waters of that Contracting Government;

.3 inspection of the ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter; or

.4 denial of entry into port.

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

3 Additional provisions

3.1 In the event:

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

.2 any of the steps referred to in paragraph 2.5 are taken, an officer duly authorized by the Contracting Government shall forthwith inform in writing the Administration specifying which control measures have been imposed or steps taken and the reasons thereof. The Contracting Government imposing the control measures or steps shall also notify the recognized security organization, which issued the Certificate relating to the ship concerned and the Organization when any such control measures have been imposed or steps taken.

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

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

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

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

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

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

Regulation 10

Requirements for port facilities

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

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

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

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

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

Regulation 11

Alternative security agreements

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

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

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

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

Regulation 12
Equivalent security arrangements

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

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

Regulation 13
Communication of information

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

.1 the names and contact details of their national authority or authorities responsible for ship and port facility security;

.2 the locations within their territory covered by the approved port facility security plans.

.3 the names and contact details of those who have been designated to be available at all times to receive and act upon the ship-to-shore security alerts, referred to in regulation 6.2.1;

.4 the names and contact details of those who have been designated to be available at all times to receive and act upon any communications from Contracting Governments exercising control and compliance measures, referred to in regulation 9.3.1; and

.5 the names and contact details of those who have been designated to be available at all times to provide advice or assistance to ships and to whom ships can report any security concerns, referred to in regulation 7.2;

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

2 Contracting Governments shall, not later than 1 July 2004, communicate to the Organization the names and contact details of any recognized security organizations authorized to act on their behalf together with details of the specific responsibility and conditions of authority delegated to such organizations. Such information shall be updated as and when changes relating thereto occur. The Organization shall circulate such particulars to other Contracting Governments for the information of their officers.

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

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

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

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

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

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

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

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

.3 the periodicity of review of the agreement;

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

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

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

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

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