International Maritime Organization

E

MARITIME SAFETY COMMITTEE
89th session
Agenda item 4

MSC 89/INF.13
5 March 2011
ENGLISH ONLY

MEASURES TO ENHANCE MARITIME SECURITY

Maritime Security Manual –
Guidance for port facilities, ports and ships

Submitted by Canada

	SUMMARY
Executive summary:	This document provides the complete text of the Maritime Security Manual, incorporating revisions by the correspondence group on the review of the Maritime Security Manual developed by the Secretariat
Strategic direction:	6.1
High-level action:	6.1.1
Planned output:	6.1.1.1
Action to be taken:	Paragraph 4
Related documents:	MSC 88/26, paragraphs 4.26 to 4.28 and 4.34 to 4.41; and MSC 89/4/1

Background

1   At MSC 88, the Committee noted that the Secretariat was in the process of developing a companion manual to the ISPS Code, intended to assist SOLAS Contracting Governments in the implementation and verification of compliance with and enforcement of the provisions of SOLAS chapter XI-2 and the ISPS Code, as well as to serve as a single-source aid and reference for those engaged in delivering capacity-building activities in the field of maritime security. The Committee was informed that the draft manual was in an advanced stage of development, but would benefit from a peer review in order to ensure its completeness and accuracy.

2   The Committee therefore endorsed the recommendation of the Secretariat that a correspondence group be formed, under the coordination of Canada and the United States, to make further improvements to the draft manual between MSC 88 and MSC 89, at which session the draft manual could be approved.

PIRACY

Discussion

3   The annex contains the manual as edited following review by the correspondence group, as described in document MSC 89/4/1.

Action requested of the Committee

4   The Committee is invited to forward the attached document, with document MSC 89/4/1, to the Working Group on Maritime Security including Piracy and Armed Robbery against Ships, with a view to finalizing the Maritime Security Manual for Committee approval at this session.

***

ANNEX

MARITIME SECURITY MANUAL –

GUIDANCE FOR PORT FACILITIES, PORTS AND SHIPS

Maritime Security Manual: Guidance for port facilities, ports and ships

V2.2 – Revised draft incorporating comments from Correspondence Group, 07 March 2011

Disclaimer

This manual has been developed to consolidate existing IMO maritime security-related material into an easily read companion guide to SOLAS chapter XI-2 and the ISPS Code in order to assist States in promoting maritime security through development of the requisite legal framework, practices, procedures and material, technical and human resources. It is intended both to assist SOLAS Contracting Governments in the implementation, verification of compliance with, and enforcement of the provisions of SOLAS chapter XI-2 and the ISPS Code, and to serve as an aid and reference for those engaged in delivering capacity-building activities in the field of maritime security.

While the guidance in this Manual was developed with input from international maritime security practitioners and is based on generally recognized maritime security practices and procedures, the suggested practices and procedures are not the only means of implementing the Maritime Security Measures of SOLAS chapter XI-2 and the ISPS code. Other methods of meeting the requirements may be equally appropriate. It is also recognized that because of the diversity of legal and administrative structures within individual states, the practices and procedures proposed in the text may need to be varied to fit within such structures.

Guidance within this Manual should not be interpreted as supplanting or negating the maritime security requirements of individual states, which should take precedence over any non-mandatory guidance included herein.

Foreword

In the wake of the tragic events of 11 September 2001 in the United States of America, a Diplomatic Conference on Maritime Security was held at the London headquarters of the International Maritime Organization (IMO) from 9 to 13 December 2002. This Conference adopted a number of amendments to the International Convention for the Safety of Life at Sea, 1974, the most far-reaching of which enshrined the new International Ship and Port Facility Security (ISPS) Code. The Conference also adopted a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the ISPS Code and pave the way for future work on the subject.

The ISPS Code was produced in just over a year by the IMO's Maritime Safety Committee (MSC) and its Maritime Security Working Group. It contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B).

Due to the urgent need to have security measures in place, the ISPS Code came into effect on July 1, 2004 just 18 months after its adoption. To assist Contracting Governments in exercising their implementation responsibilities, particularly those in lesser developed countries, one of the resolutions at the Diplomatic Conference invited the IMO to develop training materials and, if necessary, further guidance on various aspects of the ISPS Code. This was accomplished in the 2003-08 period through the development of model training courses; issuance of specific guidance mainly in the form of MSC Circulars; the organization of over 100 regional and national workshops; and the conduct of several advisory and assessment missions in response to requests from individual governments.

In 2009, as the IMO's focus was shifting to other pressing security issues notably piracy and armed robbery and the implementation of Long Range Identification and Tracking systems, there was a growing recognition of the need to reinforce ISPS Code implementation and to strengthen linkages with other IMO initiatives. In responding to this need, the IMO took stock of the training and guidance materials that it had issued over the preceding six years. It found that, while some of the materials had become out-dated, much remained relevant but was situated in an array of documentation that was not easily accessible by maritime security practitioners.

This manual has been prepared as a practical way of providing government and industry practitioners responsible for implementing the ISPS Code with a consolidated and up-to-date source of guidance material with appropriate linkages to other ongoing IMO initiatives.

3

5

Section 1 Introduction

1.1   Purpose of the Manual

1.1.1   This Manual is intended to provide consolidated guidance on the implementation of the security-related amendments to the International Convention on the Safety of Life at Sea, 1974 (SOLAS Convention) which were adopted in December 2002. These amendments included a new Chapter XI-2 in the SOLAS Convention "Special measures to enhance maritime security" which enshrined the International Ship and Port Facility Security (ISPS) Code. Throughout this manual, these are collectively referred to as the Maritime Security Measures.

1.1.2   The guidance in the Manual is addressed primarily to all:

    a   Government officials who exercise the responsibilities that the Maritime Security Measures place on Contracting Governments;

    b   Port facility employees who exercise the responsibilities that the Maritime Security Measures place on port facilities; and

    c   Shipping company employees, including shipboard personnel, who exercise the responsibilities that the Maritime Security Measures place on shipping companies and their ships.

1.1.3   The guidance may also be relevant to those responsible for, or undertaking, any security-related responsibility at port facilities, in ports and on ships.

1.2   Structure

1.2.1   The Manual is presented in five Sections.

    a   Section 1: describes the purpose and content of the Manual and provides an overview of the Maritime Security Measures, outlines the benefits and challenges in their implementation and the need to maintain security awareness;

    b   Section 2: provides guidance on the security responsibilities that the Maritime Security Measures place on Governments and those who may be authorized to undertake a Government's security responsibilities;

    c   Section 3: provides guidance on the security responsibilities that the Maritime Security Measures place on port facilities and those undertaking these responsibilities at port facilities;

    d   Section 4: provides guidance on the security responsibilities that the Maritime Security Measures place on shipping companies and those undertaking these responsibilities within companies and on their ships; and

    e   Section 5: describes a security assessment methodology for port facilities and ports.

1.2.2   Each section contains a series of sub-sections corresponding to the main areas of security responsibility. Each sub-section can be further broken down to address specific responsibilities. Where appropriate, the text in each sub-section reflects the experience of Contracting Governments in implementing the maritime security measures; appendices are used to supplement the short narrative by providing references, templates, checklists, practices and methodologies that have been adopted by Contracting Governments.

1.2.3   In order to achieve a clear distinction between the mandatory provisions of the Maritime Security Measures and supporting guidance material, attention has been paid throughout the manual to the consistent use of verbs as follows:

    a   mandatory text uses 'must' or 'is/are required to', as appropriate; and

    b   guidance text uses 'should', 'could' or 'may' as appropriate.

1.2.4   The manual is to be reviewed and updated on a regular basis.

1.2.5   Many aspects of the Maritime Security Measures have responsibilities for governments, port facility operators and ship operators. To assist with understanding how these responsibilities complement each other, Appendix 1.1 identifies their location in Sections 2-4 of the manual.

1.3 Sources

1.3.1 The guidance in the Manual is mainly drawn from IMO sources. In addition to Part B of the ISPS Code, they include a variety of resolutions, circulars and circular letters. A full list is provided in Appendix 1.2 – IMO Guidance Material on Maritime Security Measures, 1986-2011. These documents are on the IMO's website and may be accessed at: www.imo.org/OurWork/Security/docs/Pages/Docs.aspx

1.3.2 Other sources of guidance material include:

    a   The ILO/IMO Code of Practice on Port Security;

    b   Presentations at IMO regional and national workshops;

    c   Internet sites of Contracting Governments and their multi-lateral organizations; and

    d   Information made available to the IMO by Contracting Governments on their organizational structures, practices and procedures; the guidance issued to their port facilities and shipping companies; and their implementation experience.

1.3.3 To a lesser extent, elements of the guidance in the Manual is derived from material on the internet sites of Non-Governmental Organizations representing the ports and shipping industries, and individual port authorities and shipping companies.

1.3.4 To the extent possible, the Manual's contents include illustrative examples drawn from the sources described above.

1.4 Overview of the Maritime Security Measures

Origins

1.4.1 After the 1985 attack on the Achille Lauro, the Maritime Safety Committee (MSC) issued guidance on the security of cruise ships and the ports that they use. The guidance covered:

    a   The appointment within Government of a Designated Authority responsible for cruise ship and cruise port security;

    b   The appointment of an Operator Security Officer by shipping companies operating cruise ships;

    c   The appointment of a Ship Security Officer for each cruise ship;

    d   Undertaking a Ship Security Survey of each cruise ship;

    e   Preparation of a Ship Security Plan for each cruise ship and its approval by a Designated Authority within Government;

    f   Appointment of Facility Security Officers at cruise ports;

    g   Undertaking a Facility Security Survey for each cruise port; and

    h   Preparation of a Facility Security Plan for each cruise port and approval by the Designated Authority.

1.4.2 Some Governments imported elements of this guidance into their national legislation.

1.4.3 In 1996, the MSC extended the application of the above guidance to international passenger ferry services and the ports that they use. This further guidance recommended the use of three threat levels:

    a   Background;

    b   Moderate; and

    c   High.

1.4.4 In November 2001, the IMO issued a resolution which called for a review of the existing international legal and technical measures to prevent and suppress terrorist acts against ships at sea and in port, and to improve security aboard and ashore. The aim was to:

    a   Reduce risks to passengers, crew and port personnel on board ships and in port areas as well as to ships and their cargos;

    b   Enhance ship and port security; and

    c   Prevent shipping from becoming a target of international terrorism.

1.4.5   In December 2002, a Diplomatic Conference on Maritime Security was held at the London headquarters of the IMO. It was attended by 109 Contracting Governments to the SOLAS Convention (see below) and observers from other United Nations agencies, intergovernmental organizations and non-governmental international associations. Its work resulted in the adoption of the SOLAS Amendments 2002 (see below).

The SOLAS Convention

1.4.6   The 1974 SOLAS Convention is one of 32 international conventions and agreements that have been adopted by the IMO. It is the premier international treaty dealing with the safety of ships and specifies minimum standards for the construction, equipment and operation of ships. Since its adoption in 1974, the SOLAS Convention has been updated on numerous occasions

The SOLAS Amendments 2002

1.4.7   In December 2002, the IMO adopted security-related amendments to the SOLAS Convention aimed at enhancing the security of ships and the port facilities that they use. The amendments include thirteen mandatory regulations in Chapter XI-2 "Special measures to enhance maritime security" and the linked International Ship and Port Facility Security (ISPS) Code, collectively referred to as the Maritime Security Measures throughout this manual.

1.4.8   The ISPS Code has a mandatory section (Part A) and a recommendatory section (Part B). The guidance given in Part B of the ISPS Code should be taken into account when implementing the SOLAS chapter XI-2 regulations and the mandatory provisions in Part A. The IMO has published the ISPS Code, including Chapter XI-2, in English, French, Spanish and Arabic; an electronic version is also available in English, French, Spanish and Russian. Both versions may be obtained by accessing the IMO's website at: www.imo.org/Publications

Conference Resolutions

1.4.9   In addition to adopting the SOLAS Amendments 2002, the Diplomatic Conference considered a range of maritime security issues and adopted nine Conference resolutions addressing:

a   Further work by the International Maritime Organization pertaining to the enhancement of maritime security;

b   Future amendments to Chapters XI-1 and XI-2 of the 1974 SOLAS Convention on special measures to enhance maritime safety and security;

c   Promotion of technical co-operation and assistance;

d   Early implementation of the special measures to enhance maritime security;

e   Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling units on location and fixed and floating platforms not covered by chapter XI-2 of the 1974 SOLAS Convention;

f   Enhancement of security in co-operation with the International Labour Organization;

g   Enhancement of security in co-operation with the World Customs Organization;

h   Early implementation of long-range ships' identification and tracking; and

i   Human element-related aspects and shore leave for seafarers.

The Maritime Security Measures in Brief

1.4.10   Most Governments have to enact national legislation to give full effect to the Maritime Security Measures. While Governments have the discretion to extend provisions from the Maritime Security Measures to ships and port facilities that the Measures do not apply to, they cannot adopt legislative provisions whose effect would be to apply lower requirements to ships and port facilities regulated under the Maritime Security Measures than those specified in the Measures.

1.4.11   The following paragraphs outline some of the key features of the Maritime Security Measures.

Organizations within Government

1.4.12   Contracting Governments can establish Designated Authorities within Government to undertake their port facility security responsibilities. Governments or their Designated Authorities and Administrations may delegate the undertaking of certain responsibilities to Recognized Security Organizations outside Government.

1.4.13   The setting of the security level applying at any particular time is the responsibility of Governments and will apply to their ships and port facilities. The ISPS Code defines three security levels for international use:

      a   Security Level 1, normal;

      b   Security Level 2, lasting for the period of time when there is a heightened risk of a security incident; and

      c   Security Level 3, lasting for the period of time when there is the probable or imminent risk of a security incident.

Information to the IMO

1.4.14   The Maritime Security Measures require certain information to be provided to the IMO and information to be made available to allow effective communication between Company/Ship Security Officers and the Port Facility Security Officers responsible for the port facility and the ships that they serve.

Risk management

1.4.15   In essence, the Maritime Security Measures were developed with the basic understanding that ensuring the security of ships and port facilities was a risk management activity and that to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. The purpose of the ISPS Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat levels with changes in vulnerability for ships and port facilities.

1.4.16   This risk management concept is embodied in the Maritime Security Measures through a number of functional security requirements for ships and port facilities including but not limited to security assessments, security plans and access control.

1.4.17   Any shipping company operating ships to which the Maritime Security Measures apply must appoint at least one Company Security Officer for the company and a Ship Security Officer for each of its ships.

1.4.18   Governments are required to undertake a Port Facility Security Assessment (PFSA) on each port facility within the scope of the Maritime Security Measures. The results have to be approved by the Government and are to be used to help determine which port facilities are required to appoint a Port Facility Security Officer (PFSO). Each PFSA should be reviewed regularly. When completed, the PFSA has to be provided to the PFSO.

Milestones

1.4.19   The Maritime Security Measures entered into force internationally on July 1, 2004.

1.4.20   Certain elements of the information that Governments must provide to the IMO must be updated and returned to the IMO at five-year intervals, first by 1 July 2009 and again by 1 July 2014. The required information is identified in sub-section 2.19.

1.5   Benefits of, and challenges in, implementing the Maritime Security Measures

1.5.1   Following adoption of the Maritime Security Measures in December 2002, Governments had until 1 July 2004 to implement the Maritime Security Measures in their national legislation and to make the necessary administrative and organizational alterations to facilitate their implementation.

1.5.2   Many Governments achieved this target, although a number of interim arrangements were required. In many cases, enhancements were made later in the light of experience.

1.5.3   A number of Governments have also applied security requirements to port facilities, port areas and ships not covered by the Maritime Security Measures. This has included extending the application to ships operating domestic services and the application of provisions taken from the IMO/ILO Code of Practice on Port Security to port areas.

1.5.4   Since the entry into force of the Maritime Security Measures, a number of port facilities have reported a marked reduction in both the incidence of thefts and the number of accidents in security restricted areas. In

addition, it has been reported that, during the first six months since the introduction of the Measures, there was a significant reduction in stowaway cases in US ports.

1.5.5   A review of the statistics published by regional Memoranda of Understanding on Port State Control indicated that security-related deficiencies found on ships to which the Maritime Security Measures apply also showed a positive trend, albeit after some difficulties in the period immediately following their introduction.

1.5.6   Maritime Security Measures were developed in response to perceived terrorist threats. However, to varying degrees, the measures are applicable to countering other forms of security threats, notably piracy and armed robbery in international and territorial waters; and unlawful activities such as drug smuggling at ports. Thus, the fundamental purpose of the ISPS Code can be considered to reduce the vulnerability of the maritime industry to security threats, regardless of their nature.

1.5.7   As with all other aspects of shipping regulated through multilateral treaty instruments, the effectiveness of the requirements is dependent on the degree to which the relevant provisions are universally implemented and enforced. Thus, the success of the Maritime Security Measures is in the hands of Governments and the shipping and port industries.

1.5.8   When the Maritime Security Measures are implemented and enforced proportionally (i.e. ensuring that the action taken 'fits' the seriousness of the contravention) and effectively, they have proved to be successful in protecting ships and port facilities from unlawful acts. However, although the Maritime Security Measures came into effect in 1 July 2004, gaps in their implementation and application persist.

1.5.9   Many Governments are still striving to fully implement the Maritime Security Measures, particularly those pertaining to port facilities, due to a variety of factors including:

   a   Competing priorities for funds – these may include anti-piracy and armed robbery measures, maritime safety & environmental protection, and security measures for the other modes of transportation;

   b   The high cost of implementing security measures at port facilities – estimated in a 2007 study by the UN Conference on Trade and Development to average US$287,000 in investment costs and US$105,000 in annual running costs per port facility;

   c   Difficulty in quantifying the effectiveness of security measures other than by means of anecdotal evidence—although a focus on such factors as fewer deaths, theft-related infractions and unauthorized entry into restricted areas may provide empirical-based measures of success;

   d   Difficulty in estimating the probability and consequences of each type of potential threat and integrating it with known vulnerabilities particularly for port facilities;

   e   The lack of the legal and policy instruments required to achieve compliance with the Maritime Security Measures and resolve jurisdictional issues between government agencies;

   f   Limitations in the training received by security practitioners - training programs should be designed by qualified personnel to meet the specific implementation responsibilities of each type of practitioner (e.g. government officials, security officers, guards, managers); and

   g   Limitations in the guidance readily accessible to security practitioners, particularly on the implementation experience of governments and the industry.

1.5.10   As the Maritime Security Measures become an accepted part of the shipping and port industries there have been reports of varying levels of diligence in their implementation. New patterns of security threats and incidents can, and have, emerged.

1.5.11   From their inception, it has been repeatedly emphasised that those implementing the Maritime Security Measures should give due regard to the welfare of seafarers, particularly with reference to seafarers access to shore and shore leave and allowing access to ships by representative of organizations committed to the welfare of seafarers. Problems in these respects can still arise and this Manual re-emphasises the IMO's collective view that the Maritime Security Measures should not be used to impose unnecessary restrictions or additional costs on seafarers.

1.5.12   This Manual is a response to these challenges by providing practitioners with a consolidated and up-to-date source of guidance material on port facility and ship security. In doing so, it recognizes the need to refocus implementation efforts and strengthen linkages with other ongoing IMO initiatives, notably:

   a   Benefits of the measures in efforts to counter piracy and armed robbery at sea;

5

b   Utility of Long range Information and Tracking systems for enhanced maritime situational awareness;

c   Role of seafarers in a security regime; and

d   Balance between facilitation of trade and security.

1.6   Maintaining security awareness

Introduction

1.6.1   Historically, the port and shipping industries experienced high levels of criminal activity, particularly smuggling and pilferage, which impeded the development of a positive security culture in the maritime industries.

1.6.2   Effective implementation of the Maritime Security Measures has given port and ship users greater confidence that their cargoes will arrive intact and without tampering. This has resulted in economic benefits to port facilities that maintain high security standards.

1.6.3   Despite this, the promotion of security awareness and the continued development of a security culture across the port and shipping industries remains a continuing challenge for all those involved in port and ship security. In order to play a leadership role, government organizations need to coordinate their efforts in meeting this challenge.

1.6.4   Security awareness is part of the training required under the Maritime Security Measures for PFSOs, those undertaking port facility security related duties and other port facility personnel.

1.6.5   Similarly, security awareness is part of the training required for Company Security Officers, Ship Security Officers and all shipboard personnel.

Security Awareness Programs

1.6.6   Promoting security awareness is vital to the security and safety and health of all port facility, port and ship personnel. For this reason, it is important that those responsible for implementing or overseeing the implementation of the Maritime Security Measures take the steps necessary to maintain and enhance security awareness among their stakeholders and employees.

1.6.7   Typically, this is achieved through awareness programs. To be successful, the designers of such programs should ask themselves the following questions:

a   What message(s) needs to be conveyed?

b   Who should receive it?

c   How should it be communicated?

d   Is follow-up required?

1.6.8   Governments generally convey broad messages to wide audiences either directly or through their national authorities e.g. information on the government's security policy, threat levels and effective security measures as well as requesting the public to exercise continuing vigilance and to report security concerns.

1.6.9   Law enforcement services issue similar messages but directed to stakeholders at the regional or local level.

1.6.10   Port facility operators, port administrators and shipping companies are likely to focus on advising their personnel about:

a   their security policy;

b   information received on specific security threats (as is appropriate to release);

c   available training courses;

d   the need to continually exercise vigilance;

e   the need and procedures to be followed for reporting unusual incidents or behaviour; and

f   the actions that should be taken into account in the event of a security incident, including taking part in security drills or exercises.

1.6.11   The means of communication can take various forms depending on the message and the intended audience.

1.6.12   General messages to wide audiences are likely to use the media whereas more specific messages are more likely to use avenues such as presentations to security committees, the delivery of customized awareness training and the issuance of promotional material (e.g. posters, pamphlets, magazine articles and DVDs).

1.6.13   It should be noted that effective communication with local communities, land-holders and small boat operators, whose past rights of access into and around port areas may now be affected by new security measures, remains a challenge for many Designated Authorities and port facility operators.

1.6.14   Follow-up and repetition are recommended practice with examples including security awareness being a standing item at security committees and the aim of regular drills and employee training days.

1.6.15   It is important to recognize that successful security awareness programs tend to be tailored to the particular needs and concerns of each group of stakeholders; conversely, multi-stakeholder programs may not be effective if the message becomes blurred or is not available in the local language.

1.6.16   A list of websites with material on security awareness is in Appendix 1.3 – Websites showing Security Awareness Programs.

1.7   Abbreviations

1.7.1   The following are abbreviations (acronyms) used in the Manual
    a   AFA – Armed Forces Authority
    b   AIS – Automatic Identification System
    c   APEC – Asia Pacific Economic Cooperation
    d   ASA – Alternative Security Agreement
    e   CCTV – Closed Circuit Television
    f   CSO – Company Security Officer
    g   CSP – Continuous Service Provider
    h   DOS – Declaration of Security
    i   EMSA – European Maritime Safety Agency
    j   ESA – Equivalent Security Arrangement
    k   FAL – IMO's Facilitation Committee
    l   FPSO – Floating Production Storage and Offloading vessel
    m   GISIS – Global Integrated Shipping Information System
    n   GMDSS – Global Maritime Distress and Safety System
    o   GNSS – Global Navigation Satellite System
    p   ID – Identification Document
    q   IDE – International Data Exchange
    r   ILO – International Labour Organization
    s   IMO – International Maritime Organization
    t   ISM – International Safety Management Code
    u   ISPS – International Ship and Port Facility Security Code
    v   ISSC – International Ship Security Certificate
    w   LRIT – Long-range Identification and Tracking system
    x   MODU – Mobile Offshore Drilling Unit
    y   MOU – Memorandum of Understanding
    z   MRCC – Maritime Rescue Co-ordination Centre
    aa   MSC – IMO's Maritime Safety Committee
    bb   OAS – Organization of American States
    cc   PFSA – Port Facility Security Assessment

dd   PFSP – Port Facility Security Plan

ee   PFSO – Port Facility Security Officer

ff   PSA – Port Security Assessment

gg   PSAC – Port Security Advisory Committee

hh   PSC – Port Security Committee

ii   PSO – Port Security Officer

jj   RO – Recognized Organization

kk   RSO – Recognized Security Organization

ll   SAFE – WCO's SAFE Framework of Standards to secure and facilitate global trade

mm   SAR – Search and Rescue

nn   SOC – Statement of Compliance

oo   SOLAS – International Convention for the Safety of Life at Sea

pp   SSA – Ship Security Assessment

qq   SSAS – Ship Security Alert System

rr   SSO – Ship Security Officer

ss   SSP – Ship Security Plan

tt   STCW – International Convention on Standards of Training, Certification and Watchkeeping for Seafarers

uu   SUA – Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

vv   UN – United Nations

ww   WCO – World Customs Organization

1.8   Definitions

1.8.1   The following definitions apply to this Manual:

a   *Administration* means the Government of the State whose flag the ship is entitled to fly. In the Maritime Security Measures and the Maritime Security Manual, "Administration" is used to describe the organization within Government responsible for ship security.

b   *Alternative Security Agreements (ASA)* means a bilateral or multilateral agreement between Governments covering short international voyages on fixed routes between dedicated port facilities, allowing the security measures and procedures applied to the port facilities and ships to differ from those required under the Maritime Security Measures.

c   *Application of the Measures* means determining the port facilities covered by the Maritime Security Measures i.e. those required to appoint a PFSO and submit a PFSP, and communicating their location along with the identity and title of their PFSO and the PFSP approval date. In cases where port facilities are occasionally used by ships on international voyages, undertaking a port facility security assessment to decide the extent of application of the Maritime Security Measures.

d   *Armed Forces Authority (AFA)* means the organization within Government responsible for co-ordinating the military or security forces response to a security incident.

e   *Certification* means issuing International Ship Security Certificates (ISSCs), Interim ISSCs and Statements of Compliance for Port Facilities (optional).

f   *Chapter* means a chapter of the SOLAS Convention.

g   *Clear grounds* means reasons for believing that a ship does not comply with requirements of the Maritime Security Measures.

h   *Company* means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management (ISM) Code.

i   *Company security officer (CSO)* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for

approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

j   *Competent Authority* means an organization designated by an Administration to receive and act on a ship-to-shore security alert.

k   *Compliance Verifications* means undertaking intermediate and renewal verifications of compliance for ISSC issuance.

l   *Continuous Synopsis Record (CSR)* is a record maintained and updated throughout a ship's life and issued by the ship's Administration under SOLAS Chapter XI-I, "Special measures to enhance maritime safety," containing information, including the name of the Administration or Contracting Government who issued the ship's current ISSC or Interim ISSC, and the name of the body who carried out the verification of which the Certificate was issued if not the Administration or Contracting Government. The original names of those who issued previous International Ship Security Certificates have to remain in the CSR.

m   *Contracting Government* generally means a Government that has agreed to be bound by any IMO Convention, e.g. the SOLAS Convention, or other binding instrument adopted by the IMO. In the Maritime Security Manual the simpler term Government is generally used in place of Contracting Government unless there is a direct quotation from SOLAS Chapter XI-2 or from the ISPS Code Part A or Part B. Depending on the context Government can also be used in the IMO Maritime Security Measures with either the term Administration or Designated Authority, or with both, or in place of either or both.

n   *Control and compliance* measures means actions that can be taken by a duly authorized officer when it is believed that clear grounds exist that a foreign-flagged ship does not comply with the requirements of the Maritime Security Measures; notifying the relevant Government when such measures have been applied to a ship, designating the contact point to receive communication from Governments exercising control and compliance measures, and communicating the contact details to the IMO.

o   *Declaration of Security (DOS)* 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.

p   *Deficiency* means a failure to comply with the requirements of the Maritime Security Measures.

q   *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. In the ILO/IMO Code of Practice on Port Security the term is used to describe the organization within Government responsible for port security.

r   *Duly authorized officer* means a Government official given specific authorization to undertake official duties, usually associated with inspection and enforcement activities. Such duties under the Maritime Security Measures include undertaking control and compliance measures in respect of foreign flagged vessels under the Maritime Security Measures and the use of the term in the Maritime Security Manual is usually associated with that activity.

s   *Emergency response services* includes police, military, fire and ambulance services responding to a security incident or an accident.

t   *Equivalent Security Agreement (ESA)* means a Designated Authority or Administration allowing a port facility, a group of port facilities or a ship to implement other security measures other than those in the Maritime Security Measures but equivalent to those in the Maritime Security Measures.

u   *Government* is used in the Maritime Security Manual in place of "Contracting Government". Depending on the context, the term may be used in the Manual with Administrations or Designated Authority, or in their place.

v   *Government official* means any Government employee who has security related responsibilities under the Maritime Security Measures and includes duly authorized officers undertaking control and compliance measures in respect of foreign flagged vessels using the Maritime Security Measures.

w   *ILO/IMO Code of Practice* means the ILO/IMO Code of Practice on Port Security.

x   *Interim International Ship Security Certificate (Interim ISSC)* is a Certificate issued by, or on behalf of, a ship's Administration for a ship without an ISSC:

- on delivery or prior to entry into service,
- following transfer between Contracting Governments to the SOLAS Convention,
- following transfer to a Contracting Government from a non-Contracting Government, or
- following a change of the company operating the ship.

y *International Safety Management (ISM) Code* means the International Management Code for the Safe Operation of Ships and for Pollution Prevention required to be carried by all SOLAS ships under SOLAS Chapter IX "Management for the safe operation of ships".

z *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) (SOLAS Chapter XI-2).

aa *International Ship Security Certificate (ISSC)* is a Certificate issued following verification by, or on behalf, of the ship's Administration that the ship complies with the requirements in SOLAS Chapter XI-2 and the ISPS Code.

bb *International voyage* means a voyage from a country to which the SOLAS Convention applies to a port outside such a country, or conversely (SOLAS Chapter I "General provisions").

cc *Maritime Security Measures* means SOLAS Chapter XI-2 "Special measures to enhance maritime security" and the ISPS Code Parts A and B.

dd *Member State* means a member State of the International Maritime Organization or International Labour Organization.

ee *Non-SOLAS port facilities* means port facilities to which the SOLAS Convention does not apply or which occasionally handle ships to which the Maritime Security Measures apply but do not have to appoint a PFSO or submit a PFSP.

ff *Non-SOLAS ship* is a ship to which the SOLAS Convention does not apply – see the definition of ship.

gg *Port* means the geographic area defined by the Government or Designated Authority, including port facilities as defined in the ISPS Code, in which maritime and other activities occur.

hh *Port facility* means 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 (SOLAS Chapter XI-2).

ii *Port facility security assessment (PFSA)* means a risk assessment undertaken by, or for a Designated Authority which is provided to Port Facility Security Officers as a prelude to the preparation of a Port Facility Security Plan or the review, or amendment, of an approved Port Facility Security Plan. A port facility security assessment also has to be undertaken by, or for, the Designated Authority for port facilities occasionally used by SOLAS ships that have not had to appoint a Port Facility Security Officer.

jj *Port facility security officer (PFSO)* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

kk *Port facility security plan (PFSP)* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

ll *Port Security Officer (PSO)* means the person tasked to manage and coordinate security in the port.

mm *Recognized security organization (RSO)* 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 the Maritime Security Measures.

nn *Regulation* means a regulation of the SOLAS Convention.

oo *Security advice and assistance:* designating a contact point to provide security advice or assistance to ships or to receive reports of security concerns from ships, and communicating contact details to the IMO.

pp *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.

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

rr   *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times.

ss   *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.

tt   *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.

uu   *Security Plans:* approving security plans submitted by port facilities (PFSPs) and shipping companies (SSPs), and any subsequent amendments.

vv   *Ship* means a passenger ship carrying more that 12 passengers or a cargo ship engaged in an international voyage and include high-speed-craft and mobile offshore drilling units MODUs. Generally, the provisions of the SOLAS Convention apply to cargo ships of, or over, 500 gross tonnes (gt). The Maritime Security Measures apply to passenger ships, as above, and to cargo ships over 500 gt. However, certain provisions from Chapter V "Safety of navigation" of the SOLAS Convention also specifically apply to cargo ships of, or over, 300 gt. including mandatory fitting of equipment associated with automatic identification systems (AIS) and long-range identification and tracking (LRIT) systems.

ww   *Shipboard personnel* means the masters and members of the crew or other persons employed or engaged in any capacity on board a ship in the business of that ship, including high-speed craft, special purpose ships and mobile offshore drilling units not on location.

xx   Shipping company: see "Company".

yy   *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.

zz   *Ship Security Alert Systems (SSAS):* provides the means by which a ship can transmit a security alert to a competent authority on shore indicating that the security of the ship is under threat or has been compromised.

aaa   *Ship security assessment* means a risk assessment undertaken by, or for, a company security officer as a prelude to the preparation of a ship security plan or the review, or amendment, of an approved Ship Security Plan

bbb   *Ship security officer (SSO)* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

ccc   *Ship security plan (SSP)* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

ddd   *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.

eee   *Short international* voyage is an international voyage in the course of which a ship is not at any time more than 200 nautical miles from a port or a place in which the passengers and crew could be placed in safety. Neither the distance between the last port of call in the country in which the voyage begins and the final port of destination, nor the return voyage, shall exceed 600 miles. The final port of destination is the last port of call in the scheduled voyage at which the ship commences its return voyage to the country in which the voyage began.

fff   *SOLAS Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.

ggg   *Threat* is the likelihood that an unlawful act will be committed against a particular target, based on a perpetrator's intent and capability. *Threat* is the likelihood that an unlawful act will be committed against a particular target, based on a perpetrator's intent and capability.

Appendix 1.1 – Cross-reference of Government and Industry Responsibilities

Maritime Security Measure (with government and industry responsibilities)	Reference in Manual to responsibilities for:		
	Government Officials	Port Facility Operators	Ship Operators
Recognized Security Organizations	2.5	3.2.5 - 3.2.8	4.2.6 - 4.2.8
Security levels	2.6	3.3	4.3
Declarations of Security	2.7	3.4	4.4
Designating port facilities	2.8.1- 2.8.9	3.2.1	-
Port facility boundaries	2.8.10 - 2.8.12	3.2.2 - 3.2.3	-
Non-SOLAS port facilities	2.8.14 - 2.8.15	3.10	-
Port Security Committees	2.8.17 - 2.8.18		4.2.5
Port Facility Security Officers	2.8.19 - 2.8.24	3.5.1 - 3.5.6	-
Port Facility Security Assessments	2.8.25 - 2.8.33	3.6	-
Port Facility Security Plans	2.8.34 - 2.8.42	3.7	-
Appointment and Qualifications of Ship Security Personnel	2.9.1 - 2.9.11	-	4.5
Ship Security Assessments	2.9.12 - 2.9.14	-	4.7
Ship Security Plans	2.9.15 - 2.9.29	-	4.8.1 - 4.8.11
Reporting security incidents	2.9.368	3.8.8 - 3.8.10	4.8.34 - 4.8.37
Security records	2.9.379	-	4.8.38 - 4.8.39
Continuous Synopsis Records	2.9.41	-	4.10.8
International Ship Security Certificates	2.10	-	4.9
Ship Security Alert Systems	2.12.4 - 2.12.15	-	4.6.1 - 4.6.11
Automatic identification systems	2.12.16 - 2.12.19	-	4.6.12- 4.6.15
Pre-Arrival Notification	2.12.20 - 2.12.24	-	4.6.13 - 4.6.15
Long Range Identification and Tracking systems	2.12.25 - 2.12.37	-	4.6.16 - 4.6.18
Alternative Security Agreements	2.13	3.2.9 - 3.2.10	4.2.9 - 4.2.11
Equivalent Security Arrangements	2.14	3.2.11	4.2.12
Control and Compliance Measures	2.11	-	4.10
Seafarer Access Considerations	2.17.6 - 2.17.10	3.8.13 - 3.8.19	4.8.30 - 4.8.33
Non-SOLAS Vessels	2.18.3 - 2.18.15	-	4.11
Port Security	2.18.16 - 2.18.20	3.9	-

Category and identifier	Full title	Adopted
AIS		
Resolution A.956(23)	Amendments to the Guidelines for the onboard operational use of ship borne automatic identification systems (AIS) (Resolution A.917(22))	26-Feb-04

Category and identifier	Full title	Adopted
Continuous Synopsis Record (CSR)		
Resolution A.959(23)	Format and guidelines for the maintenance of the Continuous Synopsis Record (CSR)	04-Mar-03
Resolution MSC.198(80)	Adoption of amendments to the Formant and Guidelines for the Maintenance of the Continuous Synopsis Record (CSR)(Resolution A.959(23))	20-May-05

Category and identifier	Full title	Adopted
Control and Compliance Measures		
MSC/Circ.1113	Guidance to port State control officers on the non-security related elements of the 2002 SOLAS amendments	07-Jun-04
MSC.1/Circ.1191	Further reminder of the obligation to notify flag States when exercising control and compliance measures	30-May-06

Category and identifier	Full title	Adopted
Facilitating secure trade		
MSC-FAL.1/Circ.1	Securing and Facilitating International trade	21-Oct-07

Category and identifier	Full title	Adopted
ILO/IMO Code of Practice on Security in Ports		24-Dec-03

Category and identifier	Full title	Adopted
LRIT		
Resolution MSC.263(84)	Revised performance standards and functional requirements for the long-range identification and tracking of ships	16-May-08
Resolution MSC.211(81)	Arrangements for the timely establishment of the Long‑range identification and tracking system	19-May-06
Resolution MSC.242(83)	Use of the Long-range Identification and Tracking Information for Maritime Safety and Marine Environment Protection Purposes	12-Oct-07
Resolution MSC.243(83)	Establishment of International LRIT Data Exchange on an interim basis	12-Oct-07
Resolution MSC.254(83)	Adoption of amendments to the Performance standards and functional requirements for the Long-range identification and tracking of ships	12-Oct-07
Resolution MSC.298(87)	Establishment of a distribution facility for the provision of LRIT information to security forces operating in waters of the Gulf of Aden and the Western Indian Ocean to aid their work in the repression of piracy and armed robbery against ships (the distribution facility)	21-May-10
MSC.1/Circ.1259/Rev.3	Long-range identification and tracking system - Technical documentation (Part I)	21-May-10
MSC.1/Circ.1294/Rev.2	Long-range identification and tracking system - Technical documentation (Part II)	15-Feb- 11
MSC.1/Circ.1295	Guidance in relation to certain types of ships which are required to transmit LRIT information, on exemptions and equivalents and on certain operation matters	08-Dec-08

MSC.1/Circ.1298	Guidance on the implementation of the LRIT system	08-Dec-08
MSC.1/Circ.1307	Guidance on the survey and certification of compliance of ships with the requirement to transmit LRIT information	09-June-09
MSC.1/Circ.1308	Guidance to search and rescue services in relation to requesting and receiving LRIT information	09-June-09
MSC.1/Circ.1376	Continuity of service plan for the LRIT system	03-Dec-08
MSC.1/Circ.1377	List of application service providers authorized to conduct conformance tests and issue LRIT Conformance test reports on behalf of the Administrations	06-Dec-10
MSC 86/INF.16	LRIT Data Distribution Plan - Accessing and entering information Guidance notes for Contracting Governments Developmental and integration testing Guidance notes for LRIT Data Centres	26-May-09

Ship Security Alert System (SSAS)		
Resolution MSC.136(76)	Performance standards for a ship security alert system	11-Dec-02
Resolution MSC.147(77)	Adoption of the Revised performance standards for a ship security alert system	29-May-03
MSC/Circ.1072	Guidance on provision of ship security alert systems	26-Jun-03
MSC/Circ.1109/Rev.1	False security alerts and distress/security double alerts	14-Dec-04
MSC/Circ.1155	Guidance on the message priority and the testing of ship security alert systems	23-May-05
MSC.1/Circ.1190	Guidance on the provision of information for identifying ships when transmitting ship security alerts	30-May-06

Maritime Rescue Co‑ordination Centres (MRCCs)		
MSC/Circ.1073	Directives for Maritime Rescue Co‑ordination Centres (MRCCs) on acts of violence against ships	10-Jun-03

Maritime Terrorism		
Resolution A.924(22)	Review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships	20-Nov-01

Non-SOLAS ships		
MSC.1/Circ.1283	Non-mandatory guidelines on security aspects of the operation of vessels which do not fall within the scope of SOLAS chapter XI‑2 and the ISPS Code	22-Dec-08

Port Security		
MSC/Circ.1106	Implementation of SOLAS chapter XI-2 and the ISPS Code to port facilities	29-Mar-04

Recognized Security Organization		
MSC/Circ.1074	Interim Guidelines for the authorization of RSOs acting on behalf of the Administration and/or Designated Authority of a Contracting Government	10-Jun-03

Training of seafarers and port personnel		
Resolution A.955(23)	Amendments to the Principles on Safe Manning (Resolution A.890(21))	26-Feb-04
MSC/Circ.1154	Guidelines on training and certification for company security officers	23-May-05
Resolution MSC.203(81)	Adoption of amendments to the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended	18-May-06
Resolution MSC.209(81)	Adoption of amendments to the Seafarers' Training, Certification and Watchkeeping (STCW) Code	18-May-06
MSC.1/Circ.1188	Guidelines on training and certification for port facility security officers	22-May-06
STCW.6/Circ.9	Amendments to Part B of the Seafarers' Training, Certification and Watchkeeping (STCW) Code	22-May-06
MSC.1/Circ.1235	Guidelines on security-related training and familiarization for shipboard personnel	21-Oct-07
MSC.1/Circ.1341	Guidelines on security-related training and familiarization for Port facility personnel	21-Oct-07
IMO Model Course 3.19	Ship Security Officer	
IMO Model Course 3.20	Company Security Officer	
IMO Model Course 3.21	Port Facility Security Officer	

Security-related Information		
MSC.1/Circ.1305	Revised guidance to masters, Companies and duly authorized officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port	09-Jun-09

Shore leave		
MSC.1/Circ.1342	Reminder in connection with shore leave and access to ships	27-May-10

Smuggling of Drugs		
Resolution A.985(24)	Revision of the Guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic (Resolution A.872(20))	06-Feb-06
Resolution FAL.9(34)	Revised Guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic	07-Dec-06

Special Purpose Ships		
MSC/Circ.1157	Interim scheme for the compliance of certain cargo ships with the special measures to enhance maritime security	23-May-05
MSC.1/Circ.1189	Interim scheme for the compliance of special purpose ships with the special measures to enhance maritime security	30-May-06

SOLAS Chapter XI-2 and the ISPS Code		
MSC/Circ.1067	Early implementation of the special measures to enhance maritime security	28-Feb-03
MSC/Circ.1097	Guidelines for the implementation of SOLAS chapter XI-2 and the ISPS Code	06-Jun-03
Circular Letter No. 2514	Information required from SOLAS Contracting Governments under the provisions of SOLAS regulation XI-2/13	08-Dec-03
MSC/Circ.1104	Implementation of SOLAS chapter XI-2 and the ISPS Code	15-Jan-04
Circular Letter No. 2529	Information required from SOLAS Contracting Governments under the provisions of SOLAS regulation XI-2/13.1.1 on communication of a single national contact point	12-Feb-04
MSC/Circ.1110	Matters related to SOLAS regulations XI-2/6 and XI-2/7	07-Jun-04
MSC/Circ.1111	Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code	07-Jun-04
MSC/Circ.1132	Guidance relating to the implementation of SOLAS chapter XI-2 and of the ISPS Code	14-Dec-04
Resolution MSC.194(80)	Adoption of amendments to the International Convention for the Safety of Life at Sea, 1974 as amended relates to the amendments (related aspects only)	20-May-05
Resolution MSC.196(80)	Adoption of amendments to the International Code for the Security of Ships and of Port Facilities (International Ship and Port Facility Security (ISPS) Code)	20-May-05
MSC/Circ.1156	Guidance on the access of public authorities, emergency response services and pilots onboard ships to which SOLAS chapter XI-2 and the ISPS Code apply	23-May-05
Resolution MSC.202(81)	Adoption of amendments to the international convention for the safety of life at sea, 1974, as amended	19-May-06
MSC.1/Circ.1194	Effective implementation of SOLAS chapter XI-2 and the ISPS Code	30-May-06

Stowaway cases		
Resolution A.871(20)	Guidelines on the allocation of responsibilities to seek the successful resolution of stowaway cases incidents	05-Dec-97
FAL.2/Circ.50/Rev.2	Reports on Stowaway incidents	29-Nov-10
Resolution A.1027(26)	Application and revision of the guidelines on the allocation of responsibilities to seek the successful resolution of stowaway cases (resolution A.871(20))	18-Jan-10

SUA Treaties (International Conference on the revision) – Final Act	19-Oct-05
Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation	01-Nov-05
Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf	01-Nov-05

Trafficking or Transport of Migrants by Sea		
MSC/Circ.896/Rev.1	Interim Measures for combating unsafe practices associated with the trafficking or transport of migrants by sea	12-Jun-01

Unlawful Acts		
Resolution A.584(14)	Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews	16-Jan-86
MSC/Circ.443	Measures to prevent unlawful acts against passengers and crews on board ships	26-Sep-86
MSC/Circ.754	Passenger ferry security	05-Jul-96

Voluntary Self-Assessment		
MSC.1/Circ.1192	Guidance on voluntary self-assessment by SOLAS Contracting Governments and by port facilities	30-May-06
MSC.1/Circ.1193	Guidance on voluntary self-assessment by Administrations and for ship security	30-May-06
MSC.1/Circ.1217	Interim Guidance on voluntary self-assessment by Companies and CSOs for ship security	14-Dec-06

Other		
Resolution MSC.160(78)	Adoption of the IMO unique company and registered owner identification number scheme	20-May-04
Resolution MSC.159(78)	Interim guidance on control and compliance measures to enhance maritime security	21-May-04
Circular Letter No. 2554	Implementation of IMO Unique Company and Registered Owner Identification Number Scheme (resolution MSC.160(78))	24-Jun-04
MSC.1/Circ.1371	List of codes, recommendations, guidelines and other safety- and security-related non-mandatory instruments	30-Jul-10

Appendix 1.3 – Websites showing Security Awareness Programs

1. America's Waterway Watch Program is a nationwide initiative that asks its members to report suspicious activity around maritime locations to local law enforcement agencies. The website for additional information is: www.americaswaterwaywatch.us/

2. Project Kraken is a regional initiative in the UK that asks local residents and maritime stakeholders to report suspicious activity around maritime locations to the local police force.   The website for additional information is: www.hampshire.police.uk/Internet/advice/kraken/

3. The Maritime and Port Authority of Singapore has produced a tri-lingual Harbour Craft Security Code poster which can be viewed at: www.mpa.gov.sg/sites/circulars_and_notices/pdfs/maritime_security_notices/pc04-18.pdf

4. The International Merchant Marine Registry of Belize has developed a set of maritime security guidelines for shipping companies which use the registry as well as a wide range of security practitioners. The 34 page document summarizes the maritime security framework in Belize; outlines the respective responsibilities of the national authority and shipping companies for implementing the Maritime Security Measures; and provides guidance on the measures to be considered in response to threats to ships and other incidents at sea. The website can be accessed at: www.immarbe.com/maritimesecurity.html

Section 2   Security Responsibilities of Governments and their National Authorities

2.1   Introduction

2.1.1   This Section provides guidance on the security responsibilities of Governments under the Maritime Security Measures. The specific topics include:

    a   Alternative Security Agreement (ASA): refer to definition in paragraph 1.8.1b;

    b   Application of the Measures: refer to definition in paragraph 1.8.1c;

    c   Certification: refer to definition in paragraph 1.8.1e;

    d   Compliance verifications: refer to definition in paragraph 1.8.1k;

    e   Continuous Synopsis Record (CSR): refer to definition in paragraph 1.8.1l;

    f   Control and Compliance Measures: refer to definition in paragraph 1.8.1n;

    g   Declaration of Security (DOS): refer to definition in paragraph 1.8.1o;

    h   Equivalent Security Arrangements (ESAs): refer to definition in paragraph 1.8.1t;

    i   Non-SOLAS port facilities: refer to definition in paragraph 1.8.1ee;

    j   Port Facility Security Assessments (PFSAs): refer to definition in paragraph 1.8.1ii;

    k   Recognized Security Organizations RSOs): refer to definition in paragraph 1.8.1mm;

    l   Security advice and assistance: refer to definition in paragraph 1.8.1oo

    m   Security Levels: refer to definition in paragraph 1.8.1qq;

    n   Security plans: refer to definition in paragraph 1.8.1uu; and

    o   Ship Security Alert Systems (SSAS): refer to definition in paragraph 1.8.1zz.

2.1.2   This section also documents the experience to date of governments in establishing their framework for implementing and overseeing the implementation of the Maritime Security Measures. Topics include:

    a   National legislation;

    b   Organizations within Government;

    c   Government co-ordination mechanisms;

    d   Port facility and ship inspections;

    e   Ship security communications;

    f   Enforcement actions;

    g   Training of Government officials with security responsibilities ;

    h   National oversight;

    i   Non-SOLAS vessels;

    j   Additional security related instruments and guidance issued by the IMO;

    k   Information to the IMO; and

    l   Wider aspects of port security.

2.1.3   Several aspects of the maritime security measures have responsibilities for both governments and port facility/ship operators. To assist with understanding how these responsibilities complement each other, the chart overleaf identifies their location within each section.

2.1.4   The IMO has encouraged Governments to assess the effectiveness with which their national authorities have fulfilled, and continue to fulfil, their obligations in respect of port facility and ship security. Implementation questionnaires issued as guidance for Designated Authorities and Administrations to examine the status of implementing their security responsibilities under the Maritime Security Measures are shown in Appendix 2.1 – Implementation Questionnaire for Designated Authorities, and Appendix 2.2 – Implementation Questionnaire for Administrations, respectively.

2.1.5   The IMO also requires Governments to provide information on their national contact points and other aspects of their responsibilities, as specified in sub-section 2.19.

Maritime Security Measure	Reference in Manual to responsibilities for:		
	Government Officials	Port Facility Operators	Ship Operators
Recognized Security Organizations	2.5	3.2.5 - 3.2.8	4.2.6 - 4.2.8
Security levels	2.6	3.3	4.3
Declarations of Security	2.7	3.4	4.4
Designating port facilities	2.8.1- 2.8.9	3.2.1	-
Port facility boundaries	2.8.10 - 2.8.12	3.2.2 - 3.2.3	-
Non-SOLAS port facilities	2.8.14 - 2.8.15	3.10	-
Port Security Committees	2.8.17 - 2.8.18	**Error! Reference source not found. - Error! Reference source not found.**	4.2.5
Port Facility Security Officers	2.8.19 - 2.8.24	3.5.1 - 3.5.6	-
Port Facility Security Assessments	2.8.25 - 2.8.33	3.6	-
Port Facility Security Plans	2.8.34 - 2.8.42	3.7	-
Appointment and Qualifications of Ship Security Personnel	2.9.1 - 2.9.11	-	4.5
Ship Security Assessments	2.9.12 - 2.9.14	-	4.7
Ship Security Plans	2.9.15 - 2.9.29	-	4.8.1 - 4.8.11
Reporting security incidents	2.9.37	3.8.8 - 3.8.10	4.8.34 - 4.8.37
Security records	2.9.38	-	4.8.38 - 4.8.39
Continuous Synopsis Records	2.9.42	-	4.10.8
International Ship Security Certificates	2.10	-	4.9
Ship Security Alert Systems	2.12.4 - 2.12.15	-	4.6.1 - 4.6.11
Automatic identification systems	2.12.16 - 2.12.19	-	4.6.12- 4.6.15
Pre-Arrival Notification	2.12.20 - 2.12.24	-	4.6.13 - 4.6.15
Long Range Identification and Tracking systems	2.12.25 - 2.12.37	-	4.6.16 - 4.6.18
Alternative Security Agreements	2.13	3.2.9 - 3.2.10	4.2.9 - 4.2.11
Equivalent Security Arrangements	2.14	3.2.11	4.2.12
Control and Compliance Measures	**Error! Reference source not found.**	-	4.10
Seafarer Access Considerations	2.17.6 - 2.17.10	3.8.13 - 3.8.19	**Error! Reference source not found.** - 4.8.33
Non-SOLAS Vessels	2.18.3 - 2.18.15	-	4.11
Port Security	2.8.17 – 2.8.19	3.9	-

2.2   National Legislation

Introduction

2.2.1   Essential to the successful implementation and oversight of the Maritime Security Measures is the drafting and enactment of appropriate national legislation. As a minimum, this should provide for the full implementation and oversight of the Maritime Security Measures.

2.2.2   A Government has the discretion to extend the application of the Maritime Security Measures, or requirements drawn from them, to the following elements under its jurisdiction (the IMO has encouraged Governments to consider such extensions to ships and port facilities and a number have done so):

     a   non-SOLAS ships;

     b   the port facilities used by non-SOLAS ships; and

     c   offshore activities.

2.2.3   The legislation should also specify the powers needed for Government officials to undertake their duties, including the inspection and testing of security measures and procedures in place at ports and port facilities and on ships, and the application of enforcement actions to correct incidents of non-compliance.

2.2.4   The term legislation encompasses all primary and secondary legislation promulgated to implement the Maritime Security Measures. Primary legislation refers to acts, laws and decrees while secondary legislation refers to regulations, instructions, orders and by-laws issued under powers granted in primary legislation.

Experience to date

2.2.5   Most Governments have enacted legislation to implement the Maritime Security Measures. The precise approach taken has depended on the specific constitutional and legislative arrangements in each country.   A number of countries have yet to put in place the legal instruments needed to fully implement the Maritime Security Measures.

2.2.6   In some countries, international legal instruments and amendments such as the Maritime Security Measures automatically apply in national law. However, in most countries the Maritime Security Measures have been implemented through the amendment of existing security, port, or shipping legislation, or through the enactment of new legal instruments.

2.2.7   For port facilities, implementation of the Maritime Security Measures has involved amendments to existing national or local port-related legislation (often in the form of port regulations or port by-laws), which already applied provisions controlling or restricting access to port areas and regulating activities within port areas..

2.2.8   Security requirements may have already been specified for ports under existing legislation relating to national security and the protection of critical national infrastructure. A number of Governments amended such legislation to incorporate the requirements in the Maritime Security Measures; in some cases, incorporation could be achieved without the need for formal amendment.

2.2.9   For ships, incorporation of the requirements in the Maritime Security Measures has been achieved through amendments to existing merchant shipping legislation which has been the means of implementing the other mandatory requirements in the SOLAS Convention.

2.2.10   A number of Governments have enacted specific new legislation to apply the requirements of the Maritime Security Measures to both their port facilities and ships. A limited number of Governments had already enacted legislation which had imposed security requirements on cruise ships using their ports.

Legislating for the Maritime Security Measures

Introduction

2.2.11   The following paragraphs provide guidance on several aspects of national legislation that could be utilized to fully implement the Maritime Security Measures.

Part B of the ISPS Code

2.2.12   While the term Maritime Security Measures, which is used throughout this manual, encompasses both parts of the ISPS Code, national legislation has generally focussed on the mandatory requirements in Part A. However, certain sections of Part A of the ISPS Code include the statement: "…taking into account the guidance given in part B of this Code".

2.2.13   A significant number of Governments have enacted legislation making significant extracts from the guidance originally provided in Part B of the ISPS Code mandatory. Some have made all the guidance in Part B mandatory.

2.2.14   Governments have taken elements from the guidance in Part B of the ISPS Code when defining the responsibilities of:

   a   national authorities and their officials including *duly authorised officers* responsible for control and compliance measures.

   b   port facility operators and their security personnel;

   c   shipping companies and their security personnel including ships' Masters; and

   d   RSOs undertaking duties for, or on behalf of, national authorities.

2.2.15   The guidance in Part B has also been used to define the processes involved when officials, port facility operators, shipping companies and their security officers are undertaking their responsibilities.

Provisions in National Legislation

2.2.16   To fully implement the requirements in the Maritime Security Measures, the legislation could cover:

   a   definitions;

   b   application;

   c   Designated Authority and Administration;

   d   Security level;

   e   port facility;

   f   port facility security assessment;

   g   ship;

   h   port facility and ship security plans;

   i   retention of records and Declarations of Security;

   j   inspection of port facilities and ships;

   k   enforcement action;

   l   control and compliance measures; and

   m   offences relating to the Maritime Security Measures.

2.2.17   The powers required for Designated Authorities and Administrations to undertake their specific responsibilities are discussed in the following paragraphs.

Definitions in Legislation

2.2.18   The definitions used in national legislation should, as far as appropriate, be similar to those used in the Maritime Security Measures. However, there are, certain terms used in the Maritime Security Measures that are not defined within them, including:

   a   Administration;

   b   shipping company;

   c   competent authority (used in connection with ship security alert systems);

   d   international voyage;

   e   Master; and

   f   restricted area.

2.2.19   It may be necessary to provide definitions for such terms in national legislation. Some are defined elsewhere in the SOLAS Convention. To the extent possible any definitions should reflect the context in which the term is found in the Maritime Security Measures. As an example the term "restricted area" could be defined as: "Restricted area means an area in a port facility or a ship that is identified as such in a port facility security plan or a ship security plan."

Application of Legislation

2.2.20   The Maritime Security Measures apply to port facilities within a State's jurisdiction, to its SOLAS ships and to its territorial sea. The Maritime Security Measures also apply to a State's overseas territories.

2.2.21   The national legislation implementing the Maritime Security Measures should define their territorial application including the State's territorial sea and, when appropriate, their extension to any overseas territory which does not have its own legislative authority.

Legislation: Designated Authority and Administration

2.2.22   The legislation could specify which organization within government is to regulate port facility security (i.e. the Designated Authority), and which organization is to regulate ship security (i.e. the Administration). Responsibility for port facility and ship security can be combined in a single organization (refer to paragraphs 2.3.1 and 2.3.2).

2.2.23   The legislation could also specify whether the organizations and their officials have delegated power to act on their own behalf, in the organization's name, or whether they act under the authority of the relevant Minister.

2.2.24   The term Designated Authority is new in the Maritime Security Measures and could be defined in national legislation. As most Governments have enacted legislation to implement earlier provisions in the SOLAS Convention and other IMO legal instruments, the term Administration may already have been defined in merchant shipping legislation.

Legislation: Security levels

2.2.25   Setting the Security level is a Government responsibility. There are few examples of national legislation that identifies the organization within Government responsible for setting it, unless it is the Designated Authority or Administration. However, national legislation could specify who is responsible for communicating changes in Security level and for receiving and responding to such changes.

2.2.26   National legislation could give the Designated Authority and Administration the power to establish the time allowed to implement a change in Security level. It could also specify the action to be taken when those responsible for:

a   communicating changes in Security level fail to do so;

b   initiating the response to such a change fail to do so within the specified time.

Legislation: Port Facilities

2.2.27   Designated Authorities need the authority to designate a port facility as:

a   one required to appoint a PFSO and prepare a PFSP; and/or

b   one used occasionally by SOLAS ships where the Designated Authority appoints an organization or person ashore to be responsible for shore-side security.

2.2.28   In the second case identified above, the Designated Authority has to undertake a PFSA.

2.2.29   National legislation could establish the requirements relating to:

a   notification to the owner or operator of a designated port facility that there is a requirement to appoint a PFSO and prepare a PFSP;

b   notification of the appointment of an organization or person ashore responsible for communicating with SOLAS ships at port facilities occasional used by such ships and the responsibilities of that organization or person; and

c   the employment status of the appointed PFSO who should either be an employee of the port facility operator or owner, or engaged on a contract or other basis by the port facility owner or operator.

2.2.30   National legislation could establish that the operator or owner of such a port facility is responsible for the actions of their PFSO and for the security of their facility.

Legislation: Port Facility Security Assessment

2.2.31   Port Facility Security Assessments are undertaken by Designated Authority officials or by recognized security organizations on their behalf. As part of the process of completing an assessment, national legislation could authorize those undertaking such assessments to:

a   enter land or premises;

b   inspect documents, records and plans; and

c   inspect security equipment.

Legislation: Ships

2.2.32   The Maritime Security Measures require shipping companies operating SOLAS ships to appoint:

a   at least one company security officer with the responsibility to undertake a ship security assessment and prepare a ship security plan for each SOLAS ship; and

b   a ship security officer responsible, accountable to the Master, for implementing the ship security plan.

2.2.33   National legislation could establish that the shipping company is responsible for the actions of their company and ship security officers and for the security of their ships.

Legislation: Port Facility and Ship Security Plans

2.2.34   The legislation could set out the requirements and the procedures applying to:

a   the submission of port facility and ship security plans;

b   the approval of port facility and ship security plans, with or without modification;

c   the requirements to review an approved port facility or ship security plan; and

d   the submission of amendments to an approved port facility or ship security plan.

Legislation: Retention of records and Declarations of Security

2.2.35   National legislation could specify the minimum time that security records and Declarations of Security have to be retained at the port facility or on a ship.

Legislation: Inspection of port facilities and ships

2.2.36   The legislation could give officials in Designated Authorities and Administrations, or those authorized to undertake inspection duties on their behalf, authority to enter port facilities or board ships to assess their compliance with the requirements of the Maritime Security Measures.

2.2.37   These powers could include the authority to:

a   inspect a port facility or ship to assess compliance;

b   inspect security equipment;

c   initiate a port facility or ship security drill;

d   enter any premises associated with a port facility or shipping company;

e   request and inspect documents, records and plans;

f   interview individuals regarding the security of a port facility or ship; and

g   obtain and retain evidence relating to a security deficiency found at a port facility or on a ship.

2.2.38   Inspections could relate to:

a   the issue or verification of a port facility's Statement of Compliance;

b   the issue of verification of a ship's International Ship Security Certificate (ISSC) or Interim ISSC; and

c   inspection, review or audit to assess the compliance of a port facility or ship with the requirements of the Maritime Security Measures.

Legislation: Enforcement action

2.2.39   The legislation could specify the actions that a Designated Authority and Administration can take if a security deficiency is found at a port facility or on a SOLAS ship.

2.2.40   If a serious deficiency is found which compromises the ability of a port facility or ship to operate at Security levels 1 to 3, the legislation should give officials the power to issue restriction or suspension notices applying to specific activities at the port facility or ships until the deficiency is corrected or until appropriate alternative security measures and procedures are in place.

2.2.41   If a security deficiency does not compromise the ability of a port facility or ship to operate at Security levels 1 to 3 and the port facility or ship fails to take action to correct the deficiency, the legislation should give officials the power to issue an enforcement notice requiring the port facility or ship to correct the deficiency within a stated period.

2.2.42   Legislation could also establish the procedures covering withdrawal of an approved PFSP or SSP and the procedure to allow their reinstatement.

2.2.43   In their legislation, many Governments provide procedures allowing port facility and ship operators to appeal the service of an enforcement notice and for such appeals to be considered. Similar rights of appeal could be considered in respect of restriction and suspension notices and the withdrawal of approved PFSPs or SSP.

2.2.44   The legislation could establish administrative, civil or criminal penalties when a port facility or ship fails to comply, for example, with an enforcement, restriction or suspension notice and procedures relating to the application of such penalties, including the right of appeal against the imposition of a penalty.

Legislation: Control and compliance measures

2.2.45   The Maritime Security Measures allow control measures to be taken when a foreign-flagged SOLAS ship is in port, or has indicated its intention to enter the port.   These control measures can involve:

  a inspection of the ship;

  b delaying the ship;

  c detention of the ship;

  d restrictions on operation;

  e expulsion from port;

  f refusal of entry into port; and

  g other lesser administrative or corrective measures.

2.2.46   The legislation could establish procedures relating to the imposition of such control measures.

2.2.47   The legislation could specify that control measures allowing expulsion from a port or refusal of entry into a port should only be applied when the ship is considered to pose an immediate security threat.

2.2.48   The Maritime Security Measures provide that compensation can be claimed if a ship is unduly detained or delayed. The legislation could establish procedures for submitting and considering claims for compensation in these circumstances.

Legislation: Offences relating to the Maritime Security Measures

2.2.49   The Maritime Security Measures do not themselves establish any offences. The criminal or terrorist acts that they seek to detect and deter are typically already offences under a State's criminal law or criminal code.

2.2.50   When implementing the Maritime Security Measures, a number of Governments have established offences in their legislation relating to:

  a failure to comply with an enforcement notice;

  b intentional obstruction or impersonation of a Government official, or other person acting on behalf of a Designated Authority or Administration;

  c failure to provide information requested by a Government official, or other person acting on behalf of a Designated Authority or Administration;

  d providing information known to be false to a Government official, or other person acting on behalf of a Designated Authority or Administration; and

  e unauthorized presence in a restricted area of a port facility or ship.

Extending the application of the Maritime Security Measures

2.2.51   The Maritime Security Measures apply to port facilities serving SOLAS ships and to SOLAS ships. Governments have been recommended to consider extending their application in appropriate circumstances to port facilities and ships that are not covered by them.

2.2.52   A number of Governments have applied requirements drawn from the Maritime Security Measures to:

a	Passenger and cargo ships solely involved in domestic voyages, including vessels involved in domestic voyages involving significant distances to overseas territories;
b	Harbour craft and other craft that interact in ship-to-ship activities with ships covered by the Maritime Security Measures;
c	Offshore supply and support vessels;
d	Fishing vessels and recreational crafts; and
e	Facilities used by the above.

2.2.53   The Maritime Security Measures do not apply to port facilities that are used primarily for military purposes. A number of Designated Authorities have applied requirements from the Maritime Security Measures to such port facilities if regular commercial services operate from them.

2.3   Organizations within Government

Organizational structures

2.3.1   The Maritime Security Measures differentiate between the roles of the Designated Authority as the organization within Government responsible for port facility security and the Administration with responsibility for ship security. It is a matter for each individual Government where the specific responsibilities of the Designated Authority and Administration are located within the Government's administrative structures.

2.3.2   Most commonly the responsibilities of the Designated Authority and the Administration are undertaken within the Departments or Ministry responsible for port and shipping matters, often a Transport Department or Ministry or within an independent governmental organization reporting to a Transport Minister. A number of Governments maintain a distinction between their Designated Authority with responsibility for port facility security and their Administration responsible for ship security. Others have combined the security responsibilities of the Designated Authority and Administration in a single organization. Occasionally the responsibilities for port facility and ship security are combined with responsibility for the security of other transport modes, including aviation.

Delegation of Responsibility

2.3.3   There are a limited number of circumstances under the Maritime Security Measures when a Designated Authority can appoint a Recognized Security Organization (RSO) to undertake duties on its behalf on port facility security. Refer to sub-section 2.55 for a list of responsibilities and conditions of delegation.

2.3.4   Delegation of ship security responsibilities is a more common practice either by Governments or their Administrations. Some Governments have chosen to delegate responsibilities to off-shore international registries albeit with oversight provided by their Transport Department or Ministry. In other instances, Administrations have delegated many of their ship security responsibilities to RSOs. Paragraphs 2.5.6-7 provide a full list of responsibilities and conditions of delegation.

2.4   Government Coordination Mechanisms

Introduction

2.4.1   Enhanced port facility, port and ship security forms part of Governments' efforts to counter terrorism and combat threats and can involve many organizations in addition to the national authorities responsible for applying the Maritime Security Measures. The main ones are listed below.

2.4.2   National Customs and Immigration Authorities undertake their own control duties at ports and on ships and have detailed knowledge of the criminal activities that they seek to detect and deter. Many of these authorities have adopted practices and procedures drawn from the WCO's Framework of Standards to Secure and Facilitate Global Trade (the SAFE Framework) applying to ports, port facilities and ships as part of the global cargo supply chain.

2.4.3   National Authorities set appropriate security levels, particularly those relating to terrorist threats, based on essential input from intelligence services and security forces authorities. Police, coast guard and military

services form a major part of a Government's response to a serious security incident and generally have their own intelligence on criminality and threats in their areas of jurisdiction. Law enforcement authorities are involved in the prosecution of offenders.

2.4.4   Decisions made by National Authorities responsible for ship and port security should be based on close co-ordination across Government and between Government organizations. This can be assisted by the establishment of an appropriate National Maritime Security Committee structure and the development of a National Maritime Security Framework or Strategy. Development of such a Framework or Strategy can avoid the possible duplication of security procedures and measures required by different Government organizations at ports and on board ships.

National Maritime Security Framework/Strategy

2.4.5   A number of Governments have developed national maritime security frameworks or strategies and policy statements. When appropriate such frameworks or strategies could be established through National legislation.

2.4.6   National maritime security frameworks or strategies provide an effective way of establishing the national context within which to understand security concerns and requirements; and provide direction and guidance on undertaking security assessments and plans. A National Maritime Security Framework/Strategy could meet the recommendation in the ILO/IMO Code of Practice on Port Security that Governments should develop a ports security policy document.

2.4.7   A National Maritime Security Framework or Strategy could cover, in appropriate detail, the following:

  a   extent and significance of the country's maritime industries and infrastructure;

  b   perception of current maritime threats;

  c   roles and responses of Government organizations;

  d   national security policies applying to ports and ships;

  e   security responsibilities of the port and shipping industries;

  f   coordination of Government and industry responses;

  g   short and longer term security priorities; and

  h   development of a security culture across the maritime industries.

National Maritime Security Committee

2.4.8   The fostering and maintenance of effective linkages between Government and industry can significantly assist the effective application of the Maritime Security Measures.

2.4.9   The work of a National Maritime Security Committee and the development, relevance and acceptability of a National Maritime Security Framework or Strategy is enhanced if appropriate arrangements are in place to consult, and involve, representatives of those regulated: the port and shipping industries, those working in ports or on ships, cargo and passenger interests.

2.4.10   Effective co-ordination at the national and port levels allows those responsible for port and ship security to gain an appreciation of the security issues and threats that they should consider in their security assessments and seek to detect and deter through the procedures and measures in their security plans. A balanced appreciation of the security risks and threats actually faced allows the development of effective, proportionate and sustainable security procedures and measures. The imposition of excessive or inappropriate security procedures and measures can reduce their acceptability and effectiveness and impose unnecessarily delays, or restrictions, on passenger or cargo movements.

2.4.11   Many Governments established national committees or working groups to co-ordinate the initial implementation of the Maritime Security Measures. While some were subsequently disbanded, several Governments formalized the arrangements and established permanent National Maritime Security Committees, or equivalents, covering the port and shipping sectors.

2.4.12   A National Maritime Security Committee can undertake two essentially interlinked activities:

  a   Assisting the coordination of port and ship security requirements across Government; and

    b   Facilitating full consultation on security issues with those regulated – the port and shipping industries, those employed at ports and on ships and those using ports and ships.

2.4.13   There are as many possible Committee structures as there are established Committees. For co-ordination within Governments, the core membership could consist of senior level representation from:

    a   Department(s)/Ministry(ies) responsible for ports and shipping;

    b   Their National Authorities;

    c   Intelligence/Security Services;

    d   National Customs and Immigration Authorities;

    e   National Police/Law Enforcement Agencies;

    f   Military (Naval) Forces;

    g   Coast Guards; and

    h   Foreign Service.

2.4.14   For consultation with all major stakeholders in the port and shipping industries, membership could be added at senior level from the national representatives of the port and shipping industries, port workers and seafarers, and cargo and passenger interests.

2.4.15   Many of these Committees have found it useful to establish specialist sub-committees or working groups to focus attention on particular security issues or initiatives. Often, stakeholder representation is to be found at the sub-committee level due to the more specific nature of the topics being addressed.

2.4.16   The terms of reference of a National Maritime Security Committee could include:

    a   identifying security threats and vulnerabilities;

    b   establishing security priorities;

    c   planning, coordinating and evaluating security initiatives;

    d   developing or contributing to a National Maritime Security Framework or Strategy;

    e   developing or contributing to government policy statements on maritime security;

    f   developing coordinated positions on meeting international obligations;

    g   addressing jurisdictional issues involving member organizations; and

    h   handling major security issues with multi-organization implications referred by high level committees.

2.4.17   Few National Maritime Security Committees have any executive authority (that rests with their member Government organizations) but their efforts have reshaped security strategies, enhancing their acceptability and effectiveness when implemented.

Participation in international and regional organizations

2.4.18   In addition to the IMO, an international organization, there are several regional organizations that have committees or sub-committees with a mandate to address issues related to implementing the Maritime Security Measures within the broader concept of maritime security, including:

    a   The Asia-Pacific Economic Cooperation (APEC) which has representation from 21 Contracting Governments in the APEC Region. Its maritime security program is administered by the Transportation Working Group whose website may be accessed at: www.apec-tptwg.org.cn/

    b   The Organization of American States (OAS) which has representation from 34 Contracting Governments throughout the Americas and the Caribbean. Its maritime security program is administered by two committees – the Inter-American Committee for Counter-Terrorism and the Inter-American Committee for Ports. Their websites may be accessed respectively at: www.cicte.oas.org/Rev/En/Programs/Port.asp and www.safeports.org/

    c   The European Maritime Safety Agency (EMSA), which has representation from 27 Contracting Governments. Its maritime security program may be accessed at: www.emsa.europa.eu

    d   The Secretariat of the Pacific Community (SPC), which has 26 members including 22 Pacific Island countries and territories. Its maritime security program may be accessed at: www.spc.int/maritime

2.5   Recognized Security Organizations

Introduction

2.5.1   Governments can authorize Recognized Security Organizations (RSOs) to undertake certain of their responsibilities under the Maritime Security Measures. Delegation of responsibilities relating to port facility security of RSOs is usually through the Designated Authority, while delegation of responsibilities relating to ship security is usually through the Administration.

2.5.2   The scope for delegating port facility security responsibilities to RSOs is restricted under the Maritime Security Measures and a limited number of Designated Authorities have authorized RSOs to undertake port facility security assessments on their behalf. A port authority or port facility operator may be appointed as a RSO undertaking duties relating to port facilities if it can demonstrate the appropriate competencies.

2.5.3   The scope for authorizing RSOs to undertake Government responsibilities for ship security is more extensive under the Maritime Security Measures than for port facility security. Many Administrations have authorized RSOs, particularly those which also have received RO status, to conduct inspections, surveys, verifications, approvals and issue Certificates for ships flying their flag under provisions elsewhere in the SOLAS and other IMO Conventions.

2.5.4   While a number of Governments have authorized RSOs to undertake certain Government responsibilities for ship and port facility security, some Governments have preferred not to authorize any RSO to undertake any of their port facility and ship security responsibilities.

2.5.5   Under the Maritime Security Measures, Governments are required to provide the IMO with the name and contact details of any RSO authorized to act on their behalf as well as details of their specific responsibilities and conditions of authority delegated to such organizations. This information can be provided using IMO's web-based database: http://gisis.imo.org, and should be kept updated.

Permitted Delegations

2.5.6   Governments may authorize a RSO to undertake the following duties:
- a   approval of SSPs and their subsequent amendments (provided that the RSO was not involved with their development or implementation);
- b   verification and certification of compliance of ships with the Maritime Security Measures;
- c   conduct of PFSAs;
- d   provision of advice and assistance on security matters including the completion of PFSAs, PFSPs, SSAs and SSPs.

2.5.7   The Maritime Security Measures specify that Governments cannot delegate any of the following duties to RSOs:
- a   setting the Security level;
- b   establishing the requirements for a Declaration of Security;
- c   determining which port facilities have to appoint a PFSO and prepare a PFSP;
- d   approving a PFSA or subsequent amendments;
- e   approving a PFSP or subsequent amendments;
- f   exercising control and compliance measures in respect of foreign-flagged SOLAS ships;
- g   approval of SSPs and subsequent amendments if they assisted in their preparation; and
- h   issuing Certificates to shipboard personnel under the STCW Convention and STCW Code.

Authorization

2.5.8   Governments should satisfy themselves that RSOs have demonstrated the organizational effectiveness and technical capabilities necessary to undertake the specific duties that may be delegated to them. These competencies are identified in Appendix 2.3 – Criteria for Selecting Recognized Security Organizations, in the form of selection criteria.

2.5.9   In keeping with sound business practices, there should be a formal written agreement signed by both parties. As a minimum, it should:

a   Specify the scope and duration of the delegation;

b   Identify the main points of contact within the national authority and the RSO;

c   Detail the procedures for communications between the national authority and the RSO;

d   Detail the oversight procedures to be used by the national authority to verify that the RSO is carrying out its delegated activities in a satisfactory manner;

e   Detail the procedures for assessing reports received from the RSO;

f   Detail the procedures to be followed by the RSO if a ship is found not to be in compliance with the regulatory requirements for which that RSO has been delegated authority;

g   Detail the procedures to be followed by the Administration and the RSO if another Government imposes control measures on a ship for which that RSO has been delegated authority for issuing the ISSC;

h   Detail the data to be provided to the national authority to assist with the authority's approval of SSPs, PFSAs and PFSPs;

i   Identify the legislation, policies, procedures and other work instruments to be provided to the RSO;

j   Specify the records to be maintained by the RSO and made available as necessary to the national authority;

k   Specify any reports to be provided on a regular basis including changes in capability (e.g. loss of key personnel); and

l   Specify a process for resolving performance-related issues.

Oversight

2.5.10   In addition to the oversight procedures identified above, Governments should ensure the adequacy and consistency of the work performed by RSOs on their behalf by establishing an oversight system that includes:

a   undertaking inspections and audits of port facilities and ships where RSOs have undertaken delegated activities; and

b   establishing requirements for certifying the RSO's quality system by independent auditors acceptable to the national authority.

2.5.11   Governments retain ultimate responsibility for the work undertaken on their behalf by the RSOs that they appoint.   They have the authority to modify or revoke their delegations to a RSO which fails to meet agreed performance standards.

Experience to date

2.5.12   Several Designated Authorities have authorized RSOs to:

a   undertake PFSAs on their behalf;

b   assist port facilities with preparing their PFSPs;

c   be training providers for PFSOs and other port facility security personnel;

d   approve training courses on port facility security by training providers or institutions other than the RSO itself.

2.5.13   Many Administrations have approved RSOs as training providers for CSOs and SSOs.

2.5.14   A number of Governments have adopted legislation requiring a review at least every five years of the performance and authorization of any RSOs to which port facility and ship security responsibilities have been delegated under the Maritime Security Measures.

2.5.15   The Maritime Security Measures require Governments to provide the names and contact details of all RSOs to which port facility and/or ship security responsibilities have been delegated and to include details of the extent or limitation of such delegations.

2.6   Security Levels

Introduction

2.6.1   The Maritime Security Measures require Contracting Governments to gather and assess information with respect to security threats which could occur at a port facility or on, or against, a SOLAS ship. This process is essential to allow their national authorities to set the appropriate security level applying to their port facilities and to ships flying their flag.

2.6.2   The term Security level refers to the degree of risk that a security incident will occur or be attempted. The Maritime Security Measures identify three levels of risk which are now used internationally:

      a   Security level 1 means the level for which minimum appropriate protective security measures shall be implemented at all times.

      b   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 the heightened risk of a security incident.

      c   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 a specific target.

2.6.3   At Security level 1, the security measures and procedures in port, port facility or ship security plans should be sufficient to counter most forms of criminality associated with ports and ships, in particular trespass, pilferage and stowaways. The priority is to allow normal commercial operations.

2.6.4   At Security level 2, the priority is also to allow the continued commercial operation of the port, port facility or ship but with increased security restrictions.

2.6.5   At Security level 3, the strictest security restrictions will be in place and could lead to the eventual suspension of commercial activities, with control of the security response transferred to the Government organizations responding to a significant incident.

2.6.6   Some national authorities have established maximum time periods in which their ports, port facilities or ships have to put in place the additional or further security procedures and measures following a change of Security level. Designated Authorities and Administrations should specify the time allowed to change to operate at a higher security level. The time period is variable depending on the reason for the change but is usually between 3 and 24 hours.

Setting the Security level

2.6.7   Many Governments use and communicate national security levels to alert the public to the perceived risk of a terrorist attack. In such cases, they may consider that the Security levels developed in the Maritime Security Measures apply only to the risk of a terrorist attack. This need not be the case. Governments may set higher Security levels to advise of the risk of other threats, particularly attacks by pirates or armed robbers against ships.

2.6.8   When a Government sets a higher Security level on grounds other than the risk of a terrorist attack, a brief statement describing the kind of threat that has led to the change could be included when it is being communicated or transmitted. Some Governments provide stakeholders with examples of the type of risks that could lead to Security levels being raised to level 2 or 3.

2.6.9   In setting the Security level applying to port facilities and ships, Governments should take account of general and specific threat information. The Maritime Security Measures consider that the factors to be considered when setting the appropriate security level are:

      a   the degree to which the threat information is credible;

      b   the degree to which the threat information is corroborated;

      c   the degree to which the threat information is specific or imminent; and

      d   the potential consequences of the threatened security incident.

2.6.10   Information on terrorist threats is likely to be held by intelligence or security services and Governments set the appropriate Security level on advice provided by such sources.   In other cases the Security level is set by the Designated Authority for ports and port facilities or by the Administration for ships based on threat information received from intelligence or security services.

2.6.11   Governments or their national authorities should only set Security level 3 for ports, port facilities or ships in exceptional circumstances when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified threat or the duration of an actual incident.

2.6.12   Governments can apply the same Security level to all their ports and port facilities. They may also apply different Security levels to groups of ports and port facilities or to parts of a port or a particular port facility. Similarly, Governments can apply the same Security level to all its ships or apply different Security levels to individual ships, types of ship, ships operating in specific sea areas or ships using specific foreign ports or port facilities.

2.6.13   Governments can apply the same Security level over their territorial sea or apply different Security levels to different parts of their territorial sea.

Communicating the Security level

2.6.14   National authorities should establish robust communication procedures to ensure that updated information on changes (both increases and decreases) in Security levels is provided without delay to their port facilities and ships and to foreign-flagged ships in or intending to enter their port facilities or intending to transit their territorial sea. The procedures should also ensure that the information reaches their own officials, particularly those that may be located in port areas.

2.6.15   If the applicable Security level is set by a national authority other than the Designated Authority or Administration, the Designated Authority or Administration still retains responsibility for the effective notification of changes in Security levels to port facilities and ships.

2.6.16   Practices for achieving robust communication procedures are:
    a   Charting the communication process;
    b   Creating and maintaining an accurate contact list for communications by means of FAX, e-mail or text message; and
    c   Regular testing.

2.6.17   Communication procedures can vary but the general practice for port facilities is that the Designated Authority provides the information to:
    a   the port security officer, or equivalent officer in the Port/Harbour Authority, in the relevant ports, who forwards the information to the PFSOs and Masters/SSOs of ships in port or intending to enter port.
    b   individual PFSOs who then pass the information to ships at or intending to use their port facility.

2.6.18   In the case of ships, some Administrations communicate changes in Security level directly to their own flag ships. Use of NAVTEX and Inmarsat-C SafetyNET allows Administrations to issue security-related messages directly to ships which are received through the ship's Global Maritime Distress Safety System (GMDSS). Administrations may also use terrestrial or satellite-based Fax transmission to communicate with ships.

2.6.19   Other Administrations provide the information to their CSOs who are then responsible for its onward transmission to ships. Occasionally, the information can be issued to CSOs and ships through the national register of ships or through RSOs. Changes in Security level have also communicated through the issue of a Notice to Mariners.

2.6.20   Under the Maritime Security Measures, Governments should establish means of communicating Security level information to foreign-flagged ships operating in their territorial sea or that have communicated their intention the enter their territorial sea. This can be done through NAVTEX, Inmarsat-C SafetyNET and sureFax. Changes to Security levels applying to all, or part, of the territorial sea can also be transmitted by Maritime Rescue Coordination Centres (MRCCs).

2.6.21   When a security risk has been identified that results in the application of a higher Security level to all or part of the territorial sea, ships that might be affected have to be able to communicate with a Contact Point ashore. This Contact Point should be available at all times to receive reports of security concerns from ships and to offer guidance to ships. The Contact Point may also receive report from port facilities of their security concerns.

2.6.22   When a higher Security level applies, the Contact Point should be in a position to:

a	advise ships operating in, or intending to enter, the territorial sea of the security procedures and measures that the coastal State considers appropriate to protect the ship from attack; and

b	inform the ship of the security measures that the coastal State has put in place to counter the identified security risk.

2.6.23	Depending on the circumstances, the Contact Point could offer advice to a ship including:

a	altering or delaying its intended passage;

b	navigating on a specified course or proceeding to a specific location;

c	the availability of security personnel or equipment that could be provided to the ship;

d	coordinating the passage, port arrival or departure of the ship to allow escort by patrol craft or aircraft; and

e	any restricted areas established by the coastal State in response to a security threat or incident.

2.6.24	Foreign-flagged ships receiving such advice have discretion as to the action they take having regard to the provisions in their ship security plan and any guidance or instructions that they may receive from their Administration.

2.6.25	Some Administrations have specified that ships flying their flag should apply the same Security level as the coastal State when transiting the State's territorial sea or operating within its Economic Exclusive Zone.

2.6.26	Contracting Governments have discretion on the extent to which they choose to exchange information on security threats with other Governments.

## 2.7	Declarations of Security

Introduction

2.7.1	A Declaration of Security (DOS) is an agreement between a port or port facility and a ship or between a ship and another ship. It confirms the security responsibilities of each party during a ship/port interface (refer to sub-section 3.4) or a ship-to-ship activity (refer to sub-section 4.4). As such, a DOS should detail what measures can be shared or additionally provided and by which party.

Establishing the requirement for a DOS

2.7.2	The Maritime Security Measures require Governments to determine when a DOS is required by assessing the risk that the ship/port interface or ship-to-ship activity poses to persons, property or the environment. These circumstances are usually specified by the Designated Authority or Administration for inclusion in port, port facility and ship security plans. They cannot be specified by RSOs.

2.7.3	The circumstances warranting a DOS can include the following scenarios:

a	a ship is operating at a higher Security level than the port facility with which it is interfacing;

b	there has been a security threat or a security incident involving a port facility or a ship with which it is interfacing;

c	a port facility or ship is operating at Security level 3;

d	there has been a change to the Security level applying to a port facility or a ship with which it is interfacing;

e	a specific ship/port interface could endanger local facilities or residents;

f	a specific ship/port interface could pose a significant pollution risk;

g	a ship/port interface involves embarking or disembarking passengers or handling of dangerous cargo;

h	a ship is using a non-SOLAS port facility;

i	a ship is undertaking a ship-to-ship activity while operating at a higher Security level than the other ship;

j	a ship is undertaking a ship-to-ship activity with a non-SOLAS ship;

k	a ship-to-ship activity involves the transfer of passengers or dangerous cargo at sea;

l	a ship-to-ship activity could involve the risk of significant marine pollution;

m	there is a Government-to-Government agreement requiring a DOS covering specified international voyages and the ships engaged on such voyages or ship-to-ship activities during such voyages;
n	a non-SOLAS ship proposes to use a SOLAS port facility.
o	the need to do so is indicated by a port facility's Designated Authority or ship's Administration;
p	a ship is not compliant with the Maritime Security Measures (e.g. without a valid ISSC).

2.7.4   The requirements to request a DOS, and those relating to the response to such requests, should be based on security considerations. Declarations of Security should never be the norm and should not normally be required when both the port facility and the ship are operating at Security level 1. Developing a matrix similar to the one shown below may be a useful way of ensuring consistency in determining when a DOS should be initiated by a port facility.

2.7.5   Developing a matrix similar to the one shown below may be a useful way of ensuring consistency in determining when a DOS should be initiated by a port facility.

Situation	Port Facility at Security Level 1	Port Facility at Security Level 2	Port Facility at Security Level 3
Non-SOLAS ship entering port facility	Required	Required	Required
	Not Required	Not Required	Not Required
Non-ISPS Code compliant ship entering port facility	Required	Required	Required
	Not Required	Not Required	Not Required
Ship at Security Level 1	Required	Required	Required
	Not Required	Not Required	Not Required
Ship at Security Level 2	Required	Required	Required
	Not Required	Not Required	Not Required
Ship at Security Level 3	Required	Required	Required
	Not Required	Not Required	Not Required
Following a security incident at port facility or on ship	Required	Required	Required
	Not Required	Not Required	Not Required
Following a threat to port facility or ship	Required	Required	Required
	Not Required	Not Required	Not Required

2.7.6   The precise circumstances when a DOS is required by a port facility from a ship can be established through the port facility security assessment. Similarly, the precise circumstances when a DOS is to be requested by a ship from a port facility or another ship can be established through the ship's security assessment.

2.7.7   Experience to date indicates that, in addition to identifying the circumstances when a DOS is to be requested, some national authorities have:

a	Specified the validity and retention periods;
b	Modified the model form issued by the IMO (refer to Appendix 3.1 – Declaration of Security Form); and
c	Permitted the use of a single DOS for multiple visits by a ship to the same facility.

Government-to-Government agreement

2.7.8   A DOS under a Government-to-Government agreement usually applies to specific voyages between two countries and to specific passenger and cargo movements between the countries when both Governments consider that the activity poses additional security risks but wish to avoid imposing a higher Security level. It is distinct from an Alternative Security Agreement which applies to short, high-frequency international voyages between adjacent countries (refer to sub-section 2.13).

Continuous Declarations of Security

2.7.9   Continuous Declarations of Security mean that a DOS is not required for each ship/port interface or ship-to-ship activity involving the same ship with the same port facility or between the same ships. In such instances, the DOS would remain in force either for a specified time or until circumstances change.

2.7.10   The circumstances under which a continuous DOS can be applied, its duration and when the DOS becomes invalid, need to be carefully defined by the relevant national authorities following security assessments of the interfaces or activities involved.

Exclusive Economic Zone and Continental Shelf

2.7.11   The Maritime Security Measures do not apply to the off-shore activities beyond a country's territorial sea but within its Exclusive Economic Zone or Continental Shelf. It is likely that SOLAS ships will operate in these waters and interface with off-shore installations and undertake ship-to-ship activities with a non-SOLAS ship. Governments have been encouraged to develop security regimes for these areas.

2.7.12   These security regimes should facilitate agreement of a DOS or equivalent agreement between a SOLAS ship and any offshore installation that it is interfacing with, including single buoy moorings, and between a SOLAS ship and any non-SOLAS ship, particularly mobile offshore drilling units on location, and floating production storage and offloading vessels (FPSOs).

Retention

2.7.13   Port facilities and ships should retain Declarations of Security for the period specified by their respective national authorities. In many cases, this is 3-5 years.

2.7.14   Ships should have any Declarations of Security established during the period covering the ship's last ten ports of call available for inspection by government officials undertaking control and compliance measures under the Maritime Security Measures (refer to sub-sections 2.11 and 4.10). This includes any DOS for a ship/port interface or ship-to-ship activity.

Request by a port facility

2.7.15   If a port facility requests a ship to agree to a DOS, the ship must comply. The PFSP will indicate the circumstances, specified by the designated authority, when such a request should be made.

Request by a ship

2.7.16   A ship can request that a DOS be agreed by a port facility or another ship. Again the circumstances when such a request should be made will be those specified by the Administration and incorporated in the SSP.

2.7.17   If a ship requests that a port facility agrees a DOS, the port facility has to acknowledge that the request was made. The port facility does not have to agree a DOS with the requesting ship unless the circumstances relating to the request conform to those in the PFSP.

2.8   Port Facility Security Responsibilities

Designating port facilities

2.8.1   Fundamental to the successful implementation of the Maritime Security Measures is the identification by the Designated Authority of all the port facilities within its territory used by SOLAS ships. The Designated Authority has to determine whether:
   a   the port facility is required to appoint a PFSO and submit, a port facility security plan (PFSP); or
   b   the port facility is occasionally used by SOLAS ships and does not have to appoint a PFSO.

2.8.2   Some Designated Authorities consider that all their port facilities used by SOLAS ships, even if the use is occasional, should appoint a PFSO and prepare a PFSP.

2.8.3   Designated Authorities have wide discretion as to how they designate their port facilities

2.8.4   Factors to be considered for determining whether a port facility occasionally used by SOLAS ships should appoint a PFSO and prepare a PFSP could include:

a   the frequency of use;

b   use by ships considered to pose a heightened security risk e.g. cruise ships or ships carrying dangerous cargoes; or

c   proximity to populated areas.

2.8.5   Most Designated Authorities have defined multiple port facilities within each of their port areas.

2.8.6   Others have defined an entire port area, often a significant area involving the entire range of shipping activities, as a single port facility.

2.8.7   One Designated Authority has determined that each port facility includes several port areas.

2.8.8   Some Designated Authorities who initially designated entire port areas as a single port facility have subsequently changed their approach to designate multiple port facilities within each port area.

2.8.9   Many Designated Authorities have categorized their port facilities based on the type of operation at the facility and consideration of the security risks that can be associated with the operation. Examples include facilities handling:

a   Cruise ships;

b   Ro-Ro passenger ships;

c   chemical, oil and gas shipments in bulk;

d   containers and Ro-Ro shipments;

e   general cargo shipments;

f   bulk cargoes (e.g. ore, coal and grain).

Port facility boundaries

2.8.10   A port facility can include an area of land or water, or land and water; it may be used either wholly or partly for the embarkation of disembarkation of passengers, or with the loading or unloading of cargo, from SOLAS ships. Essential to the designation of individual port facilities is the delineation of a clear boundary within which the port facility is responsible for exercising its responsibilities under the Maritime Security Measures. A key factor in designating individual port facilities is identifying those responsible for the ship/port interface at the facility. Usually this will be the facility operator. In multiple-use facilities, where there are a number of operators, the Designated Authority has to determine who is responsible for the overall security of the facility. This may be the owner of the facility rather than any of the operators. In water areas where control often rests with the Port Authority, or other authority, regulating the movement of ships within the port area, their designation as a distinct port facility appears to be rare.

2.8.11   How Designated Authorities have defined the extent of individual port facilities varies. Experience to date includes:

a   limiting port facilities to the land area immediately adjacent to the berth(s);

b   including all the contiguous land area, including buildings, associated with the embarkation or disembarkation of passengers or the storage, loading and unloading of cargo at the berth(s);

c   using physical features, such as tree lines, fences or lines where temporary barriers may be used;

d   recording the boundary accurately on a map and including in both the PFSA and PFSP;

e   taking responsibility for the security of water-side areas adjacent to their berth(s), particularly in relation to manoeuvring areas at oil or gas terminals where safety considerations also apply;

f   including other water areas e.g. anchorages, waiting areas and approaches from seaward;

g   including berths within port areas where harbour craft, including tugs and pilot vessels, are berthed or from which they operate;

h   including ship yards and ship repair yards;

i   including fishing ports and marinas when they are within port areas including port facilities or are immediately adjacent to a designated port facility.

2.8.12   Designated Authorities have, on occasion, not designated port facilities regularly used by SOLAS ships on the grounds that the port facility is owned and operated by a Government-appointed Ports Authority. However, such a practice does not conform to the requirements in the Maritime Security Measures.

Notification

2.8.13   Governments are required to notify the IMO of the location of port facilities within their territory that have an approved PFSP. They are required to keep the information up to date for each port facility and resubmit the information on all their facilities at least every five years. The communication of such information should be provided to IMO's GISIS database. The next date for submission of information related to port facilities with a PFSP initially approved on 1 July 2004—information related to which was required to be resubmitted by 1 July 2009—is 1 July 2014.

Non-SOLAS port facilities

2.8.14   Designated Authorities should determine what security procedures and measures are appropriate at port facilities occasionally used by SOLAS ships but where a PFSO has not been appointed.

2.8.15   Designated Authorities should appoint a person ashore with responsibility for shore-side security to liaise with SOLAS ships using the port facility. The person can be responsible for a number of non-SOLAS port facilities. The name and contact details of the person responsible for shore-side security should be made available to SOLAS ships intending to use the facility.

2.8.16   In remote areas where ships visit infrequently and there is no person ashore to take responsibility for shore-side security, the Designated Authority should rely on the visiting ships' security measures.

Port Security Committees

2.8.17   Though not required by the Maritime Security Measures, most port operators have established Port Security Committees to co-ordinate the implementation of the Maritime Security Measures in their port in a consistent manner. Many Designated Authorities have formalized these arrangements and now require Port Security Committees at their ports.

2.8.18   Guidance on the membership and roles of a Port Security Committee is in paragraphs 3.9.3 to 3.9.8.

Port Facility Security Officers

2.8.19   Port Facility Security Officers (PFSOs) appointed by, and reporting to, the management of a port facility play an essential role in establishing and maintaining the security of their port facility. Their responsibilities extend to maintaining effective communication on security matter with the Company Security Officers (CSOs) and Ship Security Officers (SSOs) of ships using, or intending to use, their port facility.

2.8.20   It is the efficiency and effectiveness of individual PFSOs working with their national and local authorities, CSOs and SSOs that underpins the continued successful application of the Maritime Security Measures.

2.8.21   The appointment of PFSOs is essentially a matter for the port facilities that are required by the Designated Authority to have a PFSO.

2.8.22   As PFSOs are likely to be entrusted with security-sensitive information, many Designated Authorities require that they are subjected to security vetting before receiving such information. This requirement should extend to other port facility personnel who perform the responsibilities of a PFSO. It can also extend to senior management at the port facility.

2.8.23   Many Designated Authorities have specified that PFSOs should undertake training courses delivered by training providers approved by the Designated Authority. Guidance on the responsibilities and training of PFSOs is in paragraphs 3.5.1 to 3.5.6.

2.8.24   National Authorities should provide guidance to PFSOs on the action to be taken on receipt of a report from a SOLAS ship in their port or port facility on the failure of the ship's security equipment or system or suspension of a security measures which compromises the ship's ability to operate at Security levels 1 to 3.

Port Facility Security Assessments

2.8.25   Designated Authorities have to ensure that a port facility security assessment (PFSA) is undertaken for each port facility.

2.8.26   PFSAs can be undertaken by the Designated Authority or by a recognized security organization authorized by the Designated Authority.

2.8.27   Guidance on undertaking port facility security assessments is in sub-section 3.6 and in Section 5.

2.8.28   When a PFSA has been completed by a recognized security organization, it has to be submitted to, and approved by, the Designated Authority. A RSO cannot approve a port facility security assessment.

2.8.29   Designated Authority personnel should have the experience and training to undertake PFSAs and to assess and approve assessments completed by RSOs.

2.8.30   When completed or approved, PFSAs should be forwarded by the Designated Authority to the PFSO for retention and to allow preparation or amendment of the PFSP.

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

2.8.32   It is for the Designated Authority to determine the frequency of review of an approved PFSA. Many Designated Authorities review them annually and when there has been a:

    a   significant security incident at the port facility;

    b   change in the shipping operations undertaken at the facility; and/or

    c   change of facility owner or operator.

2.8.33   An essential component of PFSAs undertaken for, or by, Governments and approved by them is an identification of the range of threats and security incidents that could occur. This is addressed in greater detail in Section 5.

Port Facility Security Plans

2.8.34   The development and revision of a Port Facility Security Plan (PFSP) is the responsibility of the facility's PFSO having regard to the approved PFSA. Guidance on the preparation and content of port facility security plans is provided in sub-section 3.7.

2.8.35   Designated Authorities are responsible for establishing the policies and procedures to be included in a PFSP on Declarations of Security and on the security incidents that should be reported to them and the timing of such reports. Further guidance on Declarations of Security is in sub-sections 2.7 and 3.4.

2.8.36   When completed, the draft PFSP must be submitted to, and assessed and approved by, the Designated Authority.

2.8.37   Designated Authorities should establish the procedures and timescales covering:

    a   plan preparation and submission;

    b   plan approval;

    c   amendment of approved plans; and

    d   subsequent inspections of port facilities to assess compliance with approved plans.

2.8.38   As part of the approval process, a Designated Authority can propose a modification to a submitted plan, or proposed amendment to an approved PFSP, prior to approving the submission. This could occur when the submission does not reflect the conclusions of the PFSA or there is another security issue that the Designated Authority considers to have been inadequately addressed. Such modifications should always follow consultation with the PFSO on the reasons for the modification. The procedures could involve return of the submission to the PFSO for reconsideration and its resubmission incorporating the suggested modification or alternative amendments to meet the Designated Authority's concerns.

2.8.39   Officials of Designated Authorities should have the experience and training to advise on and carry out the above procedures. To assist with approving PFSPs, Appendix 2.4 – Sample of a Port Facility Security Plan Approval Form, provides a sample form. Designated Authorities have issued guidance, in varying detail, on the content of PFSPs including, in some cases, standard templates for their plans. This guidance is described in greater detail in sub-section 3.7.

2.8.40   The PFSPs submitted for Government approval are required to include the specific security measures and procedures associated with each of the three Security levels. This may also be a requirement for port security plans but, if not, is a recommended practice for an effective plan.

2.8.41   The security plans should set out the procedures to be followed when security levels change.   While the security level applied to a port, port facility or ship may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3 and security plans should cover this possibility.

2.8.42   The use of firearms in port facilities or on or near ships can pose significant safety risks, in particular in connection with certain dangerous and hazardous substances. If Governments consider it appropriate to allow authorized armed personnel at port facilities or on board ships, steps should be taken to ensure that such personnel are duly authorized and appropriately trained in the use of their weapons and that they are aware of the risks that can arise through the discharge of weapons in port facilities or on board ship. Specific guidelines should be issued by Governments authorizing armed personnel. PFSPs should include specific guidelines on the use of weapons in the vicinity of dangerous goods or hazardous substances.

Security records

2.8.43   Designated Authorities should specify the security records that a port facility is required to keep and be available for inspection including the period for which they should be kept. The records could cover:
    a   Declarations of Security agreed with ships;
    b   security threats or incidents;
    c   changes in Security level;
    d   security training undertaken by port facility personnel;
    e   security drills and exercises;
    f   maintenance of security equipment;
    g   internal audits and reviews;
    h   reviews of port facility security assessments;
    i   reviews of the port facility security plan, and
    j   any amendments to an approved plan.

Review of an approved PFSP

2.8.44   Designated Authorities should issue guidance on the frequency of reviewing PFSPs. Often, a minimum frequency of once a year is recommended or following:
    a   a major security drill or exercise;
    b   a security threat or incident involving the port facility;
    c   a change in the shipping operations undertaken at the facility;
    d   change of the owner or operator of the facility;
    e   completion of a review of the PFSA;
    f   when an internal audit or inspection by the Designated Authority has identified failings in the facility's security organization and operations to the extent that the approved PFSP may no longer be relevant.

2.8.45   Designated Authorities adopt varying approaches when specifying the amendments that have to be submitted to them. They range from a list of a minimum number of requirements for which the Designated Authority's approval is required to a strict approach whereby any change to an approved PFSP requires their approval.

Amendments to an approved PFSP

2.8.46   Designated Authorities should notify PFSOs of the type of amendments to an approved PFSP that must be approved before they can be implemented. This notification can be provided on approval of the initial PFSP or a subsequent amendment.

2.8.47   If, under exceptional circumstances, the Designated Authority allows a PFSO to amend a PFSP without its prior approval, the amendments must be communicated to the Designated Authority at the earliest opportunity.

Internal audits

2.8.48   PFSPs should establish internal audit procedures to be followed by a port facility operator to ensure the continued effectiveness of the PFSP. To assist PFSOs, Designated Authorities could provide guidance on the following:

    a   purpose of the port facility security internal audit (e.g. to identify opportunities for improvement);

    b   frequency (e.g. once a year);

    c   audit techniques (e.g. site visits and interviews with security personnel);

    d   components of a review;

    e   sample audit report form; and

    f   selection of auditors.

Security measures and procedures

2.8.49   Designated Authorities provide guidance to each of their designated port facilities on the security measures and procedures considered appropriate at each Security level. These are based on the facility's PFSA report. Details of the measures and procedures are provided in sub-section 3.3.

2.8.50   Many Governments have classified their ports and port facilities as critical national infrastructure, or use an equivalent designation. In many cases, national standards have been developed covering the installation and maintenance of security equipment including:

    a   fencing, gates, vehicle barriers and lighting;

    b   closed circuit television (CCTV);

    c   communications and X-ray equipment;

    d   archway metal and hand held detectors;

    e   perimeter/intruder detection systems;

    f   automated access control equipment (e.g., identification readers or keypads);

    g   information and computer protection systems; and

    h   explosive trace and vapour detection equipment.

2.8.53   In such cases, Designated Authorities can refer to these national standards when advising port facilities on security equipment and equipment maintenance regimes or when inspecting them.

Statement of Compliance

2.8.51   Although it is not mandatory under the Maritime Security Measures, Designated Authorities can issue a Statement of Compliance to a port facility. It could indicate:

    a   the name the port facility;

    b   the types of ship(s) operating at the port facility;

    c   that the port facility complies with the Maritime Security Measures;

    d   the period of validity of the Statement of Compliance (which should not exceed five years); and

    e   the arrangements established by the Designated Authority for subsequent verifications of a Statement of Compliance.

2.8.52   The Maritime Security Measures contain a standard form for use by Designated Authorities (refer to Appendix 2.5 – Statement of Compliance of a Port Facility.

2.8.53   A Statement of Compliance should not be issued unless the Designated Authority has confirmed that:

    a   the port facility has a PFSA undertaken, or approved, by the Designated Authority:

      b   the port facility has a PFSP which has been duly and formally approved by the Designated Authority;

      c   the port facility's security staff have received the necessary training and can implement the security procedures in the approved PFSP; and

      d   any security equipment specified in the PFSP is in place and operating effectively.

2.8.54   A number of Designated Authorities have specified that, for a Statement of Compliance to be valid, it should have at least:

      a   an initial verification before the Statement of Compliance is first issued;

      b   one intermediate verification between the second and third anniversary of its issuance; and

      c   a renewal verification five years after first being issued.

2.8.55   As the Maritime Security Measures restrict the role of RSOs in approving PFSAs and PFSPs, it might be considered that they should not be given the authority to undertake Statement of Compliance verifications on behalf of Designated Authorities.

2.8.56   As the Maritime Security Measures restrict the role of RSOs in approving PFSAs and PFSPs, the authority to undertake Statement of Compliance verifications has generally been retained by Designated Authorities.

2.9   Ship Security Responsibilities

Appointment and qualifications of security personnel

2.9.1   Shipping companies are responsible for the appointment of CSOs, SSOs and other personnel with security duties.

2.9.2   Presently, the Maritime Security Measures provide guidance on the knowledge and training that these security personnel should have.

2.9.3   From 1 January 2012, the IMO's Standards of Training Certification and Watchkeeping (STCW) Convention and related STCW Code establish mandatory minimum requirements for security-related training and instruction for all SSOs and shipboard personnel serving on SOLAS ships. However, it does not encompass the security-related requirements for CSOs.

2.9.4   The STCW Code further stipulates that SSOs and all shipboard personnel are required to:

      a   Meet the appropriate standard of competence; and

      b   Be issued with a certificate of proficiency (which can be inspected under the control in the STCW regulations).

2.9.5   The STCW Convention and its related Code were amended at the 2010 Manila Diplomatic Conference and will enter into force on 1 January 2012. The approach taken in the amended Convention and its related Code is that of a three-layer certification process. The first layer comprises the issuance of Certificates of Competency which fall exclusively under the authority of Administrations. The second layer is that of Certificates of Proficiency which, apart from Certificates of Proficiency under regulations V/1-1 and V/1-2, can be issued on behalf of Administrations by approved training institutions. The third layer is that for Documentary Evidence that can be issued by training institutions approved by Administrations.

2.9.6   Transitional arrangements are specified for SSOs and shipboard personnel who receive security training before January 2012 including the possible need for retraining.

2.9.7   Prior to entry into force of the amended STCW Convention and Code, the IMO has advised that, as an interim measure, the ISSC should be accepted as evidence that security-related training of SSOs and shipboard personnel has been conducted in accordance with the Maritime Security Measures.

2.9.8   The STCW Code recognizes that, although shipboard personnel are not security experts, they should receive adequate security-related training so as to acquire the required competencies to perform their assigned duties and to collectively contribute to the enhancement of maritime security.

2.9.9   The STCW Code stipulates that all SSOs and shipboard personnel should receive security-related familiarization training before taking up their duties

2.9.10   Guidance on the responsibilities and qualifications of CSOs, SSOs and shipboard personnel is in sub-section 4.5.

2.9.11   Experience to date indicates that Administrations have:

    a   required their CSOs and SSOs to attend courses provided by approved training organizations;

    b   allowed CSOs to participate in the decision to appoint RSOs engaged by their shipping company in respect of its ships; and

    c   taken control measures if inspections detected a lack of security-related training.

Ship Security Assessments

2.9.12   Ship security assessments (SSAs), including the on-scene survey, are the responsibility of CSOs. Guidance on their undertaking is in sub-section 4.7.

2.9.13   Administrations are responsible for providing guidance to CSOs on the security risks that their ships may face on voyages, having regard to the ship type, the sea areas in which the ship operates, and the ports and port facilities that it uses. If a ship changes its trading pattern, the security threats that it faces may significantly change; in such cases, Administrations should be well-placed to provide revised guidance on any new threats that the ship may face as a basis for updating the SSA.

2.9.14   The Maritime Security Measures specify that the report of an up-to-date SSA should accompany, or be reflected in, ship security plans submitted for approval or when amendments to an approved plan are submitted.

Ship Security Plans

2.9.15   The development and revision of a ship security plan (SSP) is the responsibility of the shipping company's CSO having regard to the ship's approved SSA. Guidance on the preparation and content of ship security plans is provided in paragraphs 4.8.1 to 4.8.11.

2.9.16   Administrations are responsible for establishing the policies and procedures to be included in a SSP on Declarations of Security and on the security incidents that should be reported to them and the timing of such reports. Further guidance on Declarations of Security is provided in sub-section 4.4.

2.9.17   When completed, the SSP has to be submitted to, assessed and approved by, the Administration. This responsibility may be delegated to a RSO provided that the RSO has not assisted in its preparation.

2.9.18   Administrations should establish the procedures and timescales covering:

    a   plan preparation and submission;

    b   plan approval;

    c   amendment of approved plans;

    d   subsequent inspection of ships to assess compliance with approved plans.

2.9.19   As part of the approval process, an Administration can propose a modification to a submitted plan, or proposed amendment to an approved SSP, prior to approving the submission.. This could occur when the submission does not reflect the conclusions of the SSA or there is another security issue that the Designated Authority considers to have been inadequately addressed.

2.9.20   Such modifications should always follow consultation with the CSO on the reasons for the modification. The procedures could involve return of the submission to the CSO for reconsideration and its resubmission incorporating the suggested modification or alternative amendments to meet the Designated Authority's concerns.

2.9.21   An Administration's official should have the experience and training to advise on and carry out the above procedures. To assist with approving SSPs, the following website may be useful: www.dominica-registry.com. Refer to item 3 in Appendix 4.8 – Examples of Internet Sources of Guidance Material on Preparing and Validating Ship Security Plans for further details.

2.9.22 Administrations have issued guidance, in varying detail, on the content of SSPs including, in some cases, standard templates for their plans. This guidance is described in greater detail in paragraphs 4.8.1 to 4.8.11 and includes:

  a procedures for receiving changes in Security level;

  b the time allowed to move between Security levels;

  c security-related records that have to be held by the ship;

  d procedures for reporting security system and equipment failures;

  e the circumstances when a Master can refuse an inspection prior to the ship entering port by government officials under the Maritime Security Measures' control and compliance measures (sub-section **Error! Reference source not found.**);

  f responses to interdiction at sea;

  g preserving evidence following a security incident;

  h circumstances when a DOS should be requested from a port facility or other ship;

  i procedures for reporting security incidents reports to the Administration;

  j reports of internal audits and reviews of an approved SSP;

  k amendments to an approved SSP.

2.9.23 Administrations can issue guidance on the frequency of reviewing SSPs. Often, a minimum frequency of once a year is recommended or following:

  a a major security drill or exercise;

  b a security threat or incident involving the ship;

  c a change in shipping operations including the operator;

  d completion of a review of the SSA;

  e the identification, in an internal audit or inspection by the Administration, of failings in the ship's security operations, to the extent that the approved SSP may no longer be relevant.

2.9.24 A number of Administrations have provided distinct guidance to their CSOs on particular types of ships, based on their assessment of the different security risks that can be faced by the ship operators. The main types are:

  a cruise ships;

  b Ro-Ro passenger ships;

  c chemical, oil and gas tankers and produce carriers;

  d container ships;

  e Ro-Ro and general cargo ships;

  f special purpose ships and mobile offshore drilling units.

2.9.25 Ultimately, a SSP should address all the security threats that the ship may face in service and include appropriate security measures and procedures to mitigate such threats.

2.9.26 Administrations adopt varying approaches when specifying the amendments that have to be submitted to them. They range from a list of a minimum number of requirements for which the Administration's approval is required to a strict approach whereby any change to an approved SSP requires approval.

2.9.27 Administrations should notify CSOs of the type of amendments to an approved SSP that must be approved before they can be implemented. This notification can be provided on approval of the initial SSP or a subsequent amendment.

2.9.28 If the Administration allows a CSO or SSO to amend a SSP without its prior approval, the adopted amendments must be communicated to the Administration at the earliest opportunity.

2.9.29 The SSPs submitted for Government approval are required to include the specific security measures and procedures associated with each of the three Security levels. The SSPs should set out the procedures to be followed when security levels change. While the security level applied to a port, port facility or ship may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3 and security plans should cover this possibility.

2.9.30   The use of firearms on or near ships can pose significant safety risks, in particular in connection with certain dangerous and hazardous substances. If Governments consider it appropriate to allow authorized armed personnel on board ships, steps should be taken to ensure that such personnel are duly authorized and appropriately trained in the use of their weapons and that they are aware of the risks that can arise through the discharge of weapons on board ship. Specific regulations should be issued by Governments authorizing armed personnel. SSPs should include specific guidelines on the use of weapons in the vicinity of dangerous goods or hazardous substances. Firearms carried on board ship may have to be reported on arrival in port and may have to be surrendered, or held securely, for the duration of the port visit.

Reporting security system or equipment failures

2.9.31   A SSP should contain details of the procedures to be followed when the ship has to report the failure of its security equipment or system, or suspension of a security measure which compromises the ship's ability to operate at security levels 1 to 3. Such reports, together with any remedial actions that the ship proposes to take and a request for instructions, should be made immediately to the:

  a   Administration;

  b   port facility that the ship is in;

  c   the authorities of the coastal State whose territorial sea the ship is operating in or has indicated that it intends to transit.

Interdiction at sea

2.9.32   Masters have discretion to allow foreign security forces to visit their ship when in international waters. If the Master consents and an inspection establishes that an offence may have been committed, jurisdiction remains with the flag State. The flag State can transfer jurisdiction to the inspecting State. Administrations should advise their CSOs on the actions that a Master should take in response to such a request to board and inspect, for inclusion in the SSP.

2.9.33   There are an increasing number of circumstances when a ship may be boarded by foreign security forces when in international waters. These can occur under the authority of:

  a   UN Security Council Resolutions relating to the enforcement of sanctions;

  b   bilateral/multilateral agreements relating to the suppression, for example, of nuclear proliferation or drug smuggling. Such agreements are based on prior consent being given by the flag State;

  c   the IMO's 2005 Protocols to the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) Convention, which entered into force in 2010.

2.9.34   Administrations should consider providing guidance to CSOs on the actions to be taken by the ship when it is boarded under these authorities.

2.9.35   Under the SUA Convention, a request can be made by a Contracting Government to the Convention to board and inspect a ship of another Contracting Government in international waters and take appropriate measures if there are reasonable grounds for believing that a terrorist-related offence has been, is being, or is about to be committed on board. The procedure is based on prior flag State consent with jurisdiction being retained unless transferred. A ship can be detained if there is evidence that an offence has been committed. The SUA Convention allows the Master of a boarded vessel to contact the ship's Administration and the shipping company at the earliest opportunity.

Preserving evidence following a security incident

2.9.36   Administrations, in consultation with their law enforcement agencies, may wish to provide guidance to CSOs on preserving evidence found on board their ships after an incident.

Reporting security incidents

2.9.37   Administrations are required to specify the types of security incident that have to be reported to them. In such cases, they should provide guidance on their timing, procedures to be followed and their distribution. These procedures are described in greater detail in 4.8.35 to 4.8.37. They should include reporting incidents to local law enforcement agencies when in a port facility or the adjacent coastal State.

Security records

2.9.38   Administrations should specify the security records that a ship is required to keep and be available for inspection including the period for which they should be kept (refer to paragraphs 4.8.38 to 4.8.39). The records could cover:

a   Declarations of Security agreed with port facilities and other ships;

b   security threats or incidents;

c   breaches of security;

d   changes in Security level;

e   communications relating to the direct security of the ship such as specific threats to the ship or to port facilities where the ship is, or has been;

f   ship security training undertaken by the ship's personnel;

g   security drills and exercises;

h   maintenance of security equipment;

i   internal audits and reviews;

j   reviews of the ship security assessments;

k   reviews of the ship security plan, and

l   any amendments to an approved plan.

Internal audits

2.9.39   SSPs should establish internal audit procedures to be followed by a company or ship to ensure the continued effectiveness of the SSP. To assist CSOs and SSOs, Administrations could provide guidance on the following:

a   purpose of the ship security internal audit (e.g. to identify opportunities for improvement);

b   frequency (e.g. once a year);

c   audit techniques (e.g. site visits and interviews with security personnel);

d   components of a review;

e   sample audit report form;

f   selection of auditors.

Security measures and procedures

2.9.40   Administrations should provide guidance to each of their shipping companies and CSOs on the security measures and procedures considered appropriate at each Security level for their ships. These are based on the SSAs undertaken for the CSO.

2.9.41   Administrations should require that security equipment receive regular maintenance checks and that these checks be recorded. Security equipment can include:

a   closed circuit television (CCTV) and lighting;

b   communications and X-ray equipment;

c   archway metal and hand held detectors;

d   perimeter/intruder detection systems;

e   automated access control equipment;

f   information, including computer, security;

g   explosive trace and vapour detection equipment.

Continuous Synopsis Records

2.9.42   Administrations must ensure that each ship's Continuous Synopsis Record (CSR) includes the name of the:

a   Administration or RSO that issued the ship's ISSC or Interim ISSC; or

b   If different from above, the organization that carried out the verification leading to the certificate issuance.

Manning levels

2.9.43   Administrations should ensure that, when determining the safe manning level of each national ship, they take into account any additional workload that may result from the implementation of the approved SSP. Consideration should be given to the workload associated with the performance of security responsibilities, the capacity of the shipboard personnel to handle the additional workload while recognizing the need to implement the hours of rest and other measures for addressing and avoiding fatigue among ship personnel.

2.10   International Ship Security Certificates

Introduction

2.10.1   Ships falling under the Maritime Security Measures must carry either the International Ship Security Certificate (ISSC) or, in limited circumstances, the Interim ISSC, both of which are issued by their Administration.

2.10.2   Administrations inspect ships entitled to fly their flag in connection with the issue, intermediate verification and renewal of ISSCs; the issue of Interim ISSCs; and at any other time to assess the ship's compliance with the Maritime Security Measures.

2.10.3   The Maritime Security Measures contain a 'model' International Ship Security Certificate which is referenced in Appendix 2.6 – Form of the International Ship Security Certificate. If the Certificate adopted by the Administration is not in English, French or Spanish, the text should include a translation into one of those languages.

Issuance

2.10.4   An ISSC must be issued for a period specified by the Administration which, with one exception, cannot exceed five years. The exception covers the situation when a renewal verification is completed within three months of the expiry date of the existing ISSC. In this situation, the new ISSC becomes valid from the date of completion of the renewal verification to a date not exceeding five years from the expiry date of the existing ISSC.

2.10.5   An ISSC should only be issued or renewed when:
  a   the ship has an approved ship security plan indicating that it fully addresses all requirements specified in the Maritime Security measures, as outlined in paragraphs 4.8.1 to 4.8.11, and
  b   the Administration is satisfied, based on objective evidence, that the ship is operating in accordance with the provisions in the approved ship security plan.

2.10.6   A Certificate should not be issued in cases where there is a minor deviation from the ship security plan, even when the ship's ability to operate at Security levels 1 to 3 is not compromised.

2.10.7   A Certificate can be issued or endorsed by:
  a   the ship's Administration;
  b   a RSO authorized to act on behalf of the ship's Administration; or
  c   another Administration acting on behalf of the ship's Administration.

Verifications

2.10.8   SOLAS ships are subject to verifications of their compliance with the Maritime Security Measures. Verification takes place:
  a   before a ship is put into service and before the ISSC is issued – an *initial verification;*
  b   at least once between the second and third anniversary of the issuance of the ISSC if the validity period is for five years – an *intermediate verification;*
  c   before the ISSC is renewed – a *renewal verification;*
  d   at other times, at the discretion of the Administration.

2.10.9 The appropriate level of thoroughness in the verification of security systems should be as follows:

a   100% verification for all technical equipment specified in the SSP; and

b   a sample audit for all operational (non-technical) security measures, to a level necessary for the auditor to verify the whole operating system.

2.10.10 An initial verification is conducted to ensure that the ship's security system and any security equipment required by the Maritime Security Measures and the approved SSP is in satisfactory condition and fit for the service for which the ship is intended.

2.10.11 An intermediate verification is conducted to ensure that the ship's security system and any security equipment required by the Maritime Security Measures and the SSP remains in satisfactory condition and is fit for the service for which the ship is intended.

2.10.12 A renewal verification is to ensure the ship's security system and any security equipment fully complies with the requirements of the Maritime Security Measures and the approved ship security plan, is in satisfactory condition and is fit for the service for which the ship is intended.

2.10.13 After verification, the ship's security system and security equipment should be maintained to conform with the provision of the Maritime Security Measures. No changes can be made to the security system or security equipment or to the approved ship security plan unless agreed by the Administration.

Duration of validity

2.10.14 The duration of a renewed five year ISSC can vary depending on the date that the renewal verification takes place. If it is completed:

a   within the three months before the expiry of the original ISSC, then the next five-year period starts at the original expiry date;

b   after the expiry of the original ISSC, then the next five-year period starts at the original expiry date;

c   more than three months before the expiry of the original ISSC, then the next five year period starts at the date of completion of the renewal verification.

2.10.15 If an ISSC has been issued for a period of less than five years, an Administration can extend its validity to a maximum of five years after undertaking the required verification.

2.10.16 If a new ISSC cannot be placed on the ship before the original ISSC expires, the Administration can endorse the original ISSC for an extended period not exceeding five months. The new five-year period starts at the original expiry date.

2.10.17 If a ship is in transit, or its arrival at the port where verification is to take place is delayed, the Administration can endorse the original ISSC to allow the ship to complete its voyage. However, the validity period cannot be extended for longer than three months and the new five -ear period starts at the expiry date set for the original ISSC.

2.10.18 If a ship is engaged on short voyages, its ISSC can be extended for a period of up to one month with the new five-year period starting at the expiry date of the original ISSC.

2.10.19 If an intermediate verification is undertaken before the second anniversary of issuance of an ISSC that is valid for five years, its validity period must be reduced to show an expiry date that is no more than three years after the completion date of the verification. However, the original expiry date can be maintained with a further intermediate verification.

Loss of validity

2.10.20 An ISSC can lose its validity when:

a   the required intermediate and renewal verifications have not taken place;

b   it has not been endorsed following an intermediate verification;

c   a new shipping company takes over the operation of the ship; or

d   the ship changes its flag.

2.10.21   On changes of flag, the original Administration should provide the new Administration with copies of all relevant information on the ship's ISSC including copies of available verification reports.

Remedial actions

2.10.22   The ship's Administration has to be notified immediately when there is a failure of a ship's security equipment or system or suspension of a security measures which compromises the ship's ability to operate at Security levels 1 to 3. The notification should be accompanied by any proposed remedial actions.

2.10.23   The ship's Administration has also to be notified when the above circumstances do not compromise the ship's ability to operate at security levels 1 to 3. In such cases, the notification should be accompanied by an action plan specifying the alternative security measure being applied until the failure or suspension is rectified together with the timing of any repair or replacement.

2.10.24   The Administration may:
     a   approve the alternative security measures being taken and the action plan;
     b   require amendments to such measures;
     c   require additional or alternative measures,
     d   require immediate repair or replacement;
     e   take other appropriate action.

2.10.25   A ship's ISSC may be withdrawn or suspended if the alternative security measures are not applied or the approved action plan is not complied with.

2.10.26   Administrations should provide guidance to their CSOs reminding them of the cumulative effect that individual failures or suspensions of measures could have on the ability of their ships to operate at Security levels 1 to 3.

2.10.27   Administrations should also provide guidance to their officials on the action that they should take when receiving a report from a SOLAS ship on the failure of its security equipment or system or suspension of a security measures which compromises the ship's ability to operate at Security levels 1 to 3. Administrations should provide clear guidance concerning the impact of the ship's status on the validity of its ISSC.

Ship out of service

2.10.28   Administrations apply widely diverging interpretations of when a SOLAS ship is out of service or laid up; and of the circumstances and passage of time that could lead to consideration of suspension or withdrawal of the ship's ISSC.   The Maritime Security Measures do not provide specific direction on these ship out-of-service considerations.

Interim International Ship Security Certificates

2.10.29   Administrations or RSOs may issue an Interim ISSC when:
     a   a ship is on delivery, or prior to its entry or re-entry into service;
     b   a SOLAS ship is changing its flag;
     c   a ship is being transferred from a non-SOLAS State;
     d   the shipping company operating a SOLAS ship changes.

2.10.30   An Interim ISSC can only be issued when the Administration or RSO has verified that:
     a   the ship's ship security assessment has been completed
     b   there is a copy of the SSP on board;
     c   the SSP has been submitted for review and approval and is being implemented;
     d   the ship has a ship security alert system;
     e   the CSO has ensured that the necessary arrangements are in place, including drills, exercises and internal audits, for the ship to successfully complete the required verification within six months;
     f   arrangements are in place to carry out the required verification;

g   the master, SSO and other personnel with specific security duties are familiar with their responsibilities in the Maritime Security Measures and SSP and have been provided with such information in the ship's working language or in a language they understand;

h   the SSO meets the relevant requirements in the Maritime Security Measures.

2.10.31   Following verification of the items listed above, an Interim ISSC is valid for up to six months.

2.10.32   If a full ISSC is issued to the ship during that six-month period, the Interim ISSC is revoked.

2.10.33   An Interim ISSC cannot be extended.

2.10.34   The Maritime Security Measures contain a 'model' Interim ISSC that is in Appendix 2.7 – Form of the Interim International Ship Security Certificate. If the Certificate adopted by the Administration is not in English, French or Spanish, the text should include a translation into one of those languages.

2.10.35   An Administration should not issue a subsequent or consecutive Interim ISSC if it believes that the shipping company intends to avoid full compliance with the Maritime Security Measures for a period beyond the initial six-month validity of the initial Interim ISSC.

2.10.36   ISSCs and Interim ISSCs can be inspected as part of control and compliance measures described in sub-section **Error! Reference source not found.**.

Ship Inspections

2.10.37   Administrations undertake inspections of their SOLAS Ships as initial, intermediate and renewal verifications of the ship's International Ship Security Certificate. At their discretion, Administrations may also conduct:

a   additional inspections on ships flying their flag to assess compliance with the Maritime Security Measures;

b   covert tests of the Maritime Security Measures and procedures of a ship flying their flag.

2.10.38   A sample of a ship security inspection check list which can be used for verifications and other inspections is attached as Appendix 2.8 – Sample of a Ship Security Inspection Check List.

2.10.39   To assist shipping companies, Administrations and their authorized RSOs have sought to link the timing of verifications required under the Maritime Security Measures with other verifications or inspections including, particularly, those required under the ISM Code. Combining inspections in this way can be of significant benefit to the shipping industry. However, in ports where ISM auditors are not always available, this joint approach may not be practicable and could unduly delay shipping schedules.

2.10.40   The training and experience required for those undertaking verifications and inspections under the Maritime Security Measures can differ for those undertaking other forms of verification or inspection.

2.11 Control and Compliance Measures

Introduction

2.11.1   Governments can apply specific control and compliance measures to foreign flagged SOLAS ships using, or intending to use, their ports when assessing their compliance with the Maritime Security Measures. Elements of these control and compliance measures are unique including:

a   the authority to require ships to provide security related information prior to entering port;

b   the authority to inspect ships intending to enter into port when there are clear grounds for doing so once the ship is within the territorial sea, and the right of a Master to refuse such an inspection; and

c   the authority to refuse to allow a ship to enter port or to expel a ship from port.

2.11.2   Those authorized to undertake control and compliance measures under the Maritime Security Measures may also carry out control functions in respect of foreign flagged vessels under other SOLAS Convention provisions as well as under other Conventions adopted by the IMO and under International Labour Organization (ILO) Conventions. The exercise of such control measures is traditionally described as "port state control". Governments often co-operate through regional Memoranda of Understanding (MOUs) on port state control.

2.11.3   Governments should not give more favourable treatment to ships flying the flag of a State which is not a signatory of the SOLAS Convention and should apply the same control and compliance measures. However, ships that fall outside the Maritime Security Measures because of their size are subject to the measures established by the government.

2.11.4   Under the Maritime Security Measures, RSOs cannot apply control and compliance measures on behalf of Government.

Duly authorized officers

2.11.5   Governments can authorize duly authorized officers to apply the control and compliance measures under the Maritime Security Measures. Their authorization is usually through the Administration and the officers may also undertake other control functions. When undertaking their duties duly authorized officers may be assisted by specialist personnel.

2.11.6   Duly authorized officers applying control and compliance measures under the Maritime Security Measures should:

a   be knowledgeable of the Maritime Security Measures and shipboard operations;

b   be able to communicate with the ship's Master, SSO and other officers in English;

c   receive the training necessary to fully undertake the control functions that they are authorized to carry out. They may be assisted by persons with specialized search expertise;

d   receive the training necessary to ensure their proficiency in safety procedures when boarding a ship, particularly if boarding is to take place at sea. This training should specifically cover emergency evacuation procedures and procedures for entering enclosed spaces on ships;

e   when boarding a ship, carry and present identification documentation which includes their authorization to impose control measures. Procedures should be in place to allow a ship's Master or SSO to verify the identity of duly authorized officers; and

f   when on board, comply with the security measures and procedures that are in place on the ship unless they are incompatible with the control activities being undertaken.

Pre-Arrival Information Procedures

2.11.7   If requested to do so, a ship has to provide security-related information prior to entering into a port. The port State should specify the information required and provide the names and contact details of who should receive the information. This information can be assessed to establish the security risk that a particular ship may pose and to determine whether control and compliance measures should be taken in respect of the ship.

2.11.8   Most Governments have specified the minimum time before arrival in port that a ship should notify its intention to arrive and provide the necessary security-related information. The time can vary between 24 and 96 hours prior to arrival. Special arrangements may apply when ships or on short international voyage or undertake intensive short sea scheduled services on a daily basis, such as passenger Ro-Ro ferries.

2.11.9   The IMO has developed a standard data set of the security-related information that a ship might be expected to provide (refer to Appendix 4.6 – Standard Data Set of Security-related Pre-Arrival Information).   The standard data set does not preclude a Government from requesting further security-related information on a regular basis or in specified circumstances. When Governments require additional information, the shipping industry should be appropriately advised.

Clear Grounds

2.11.10   A duly authorized officer on analyzing the security-related information provided by a foreign flagged ship and any other relevant information available relating to the ship intending to enter port may consider that there are clear grounds that the ship may not in compliance with the Maritime Security Measures. Examples of such clear grounds could include:

a   evidence or reliable information that the ship has serious security deficiencies;

b   receipt of a reliable report or complaint that the ship does not comply with the requirements in the Maritime Security Measures;

c   evidence or reliable information that the ship had:

- a ship/port interface which did not comply with the Maritime Security Measures and did not take either appropriate additional security measures or complete a DOS with the port facility; or
- a ship-to-ship activity with another ship which did not comply with the Maritime Security Measures and did not take either appropriate security measures or complete a DOS with the other ship.

d   evidence or reliable information that the ship had:
- a ship/port interface which did not have to comply with the Maritime Security Measures and did not take either appropriate additional security measures or complete a DOS with the port facility; or
- a ship-to-ship activity which did not have to comply with the Maritime Security Measures and did not take either appropriate additional security measures or complete a DOS with the non-SOLAS vessel.

e   evidence that the ship holds a sequentially issued Interim ISSC contrary to the Maritime Security Measures;

f   failure of the ship to provide all of the requested security-related information identified in paragraph 2.12.20.

2.11.11   At the end of an inspection , the duly authorized officer should ensure that the ship's master or SSO is provided with a report giving the results of the inspection, details of any action taken by the officer and a list of any non-compliances to be rectified by the master, SSO or shipping company. The report should be made in accordance with the format set out in Appendix 2.14 – Report of the Imposition of a Control and Compliance Measure.

2.11.12   The duly authorized officer could at this time:
a   request the ship to rectify the non-compliance;
b   require the ship to proceed to a specified location within the territorial sea or internal waters of the port State;
c   undertake a detailed inspection of the ship, if the ship is within the territorial sea of the port State; and/or
d   deny entry into port.

2.11.13   If a deficiency is identified as a result of a detailed inspection, this could lead to the imposition of further control measures.

2.11.14   If a ship that has been advised of the intention to take control measures under the Maritime Security Measures decides to withdraw its intention to enter port, the control measures proposed by the duly authorized officer no longer apply. Any other steps that are taken in respect of the ship must be based on, and consistent with, international law.

Ship inspection in port

2.11.15   Under the Maritime Security Measures, a ship can also be inspected to assess its compliance when in port. Normally, an inspection starts with verifying the presence and validity of the ship's ISSC or Interim ISSC. A copy of a Certificate is not accepted as being a valid ISSC or Interim ISSC.

2.11.16   On the basis of observation, a duly authorized officer can establish that there are clear grounds for believing that the ship is not in compliance with the requirements of the Maritime Security Measures.

2.11.17   A duly authorized officer may not have been challenged on boarding the ship or may find that restricted areas on the ship are not secured.

2.11.18   A duly authorized officer could check:
a   that the ship is operating at the Security level applying to the port facility, or at a higher Security level set by the ship's Administration;
b   that security drills have been carried out at the required interval; and
c   the records of the last 10 ports-of-call and any ship-to-ship activity undertaken during the period of the last 10 ports-of-call.

2.11.19   Examples of clear grounds warranting an inspection could include:

  a   evidence that the ship's ISSC is not valid or has expired;

  b   evidence or observation that the ship's crew are not familiar with essential shipboard security procedures or cannot carry out ship security drills;

  c   evidence or observation that key members of the ship's crew are unable to communicate with crew members with security responsibilities.

2.11.20   The clear grounds that could apply to a ship intended to enter port could also apply to a ship in port.

2.11.21   If there are clear grounds, or no valid ISSC or Interim ISSC is on board, control measures could be applied to the ship. Any control measures must be proportionate with the identified security deficiencies. In deciding the control measures that should be applied, the duly authorized officer may consider if the ship can:

  a   maintain communication with the port facility;

  b   prevent unauthorized access to the ship and to restricted areas on the ship; and

  c   prevent the introduction of unauthorized weapons, incendiary devices or explosives to the ship.

2.11.22   If a duly authorized officer considers that the ship is not in conformity with the requirements of the Maritime Security Measures, parts of the ship's SSP may be inspected.

2.11.23   Parts of a SSP are confidential and can only be inspected by a duly authorized officer with the consent of the ship's Administration. The confidential parts of a SSP are the:

  a   identification of restricted areas and measures to prevent access to them;

  b   procedures for responding to security threats;

  c   procedures for responding to the instructions received from the ships' Administration at Security level 3;

  d   details of the duties of ship personnel with security responsibilities;

  e   procedures for inspecting, testing and calibrating security equipment on the ship;

  f   locations of the SSAS activation points; and

  g   guidance on the use of the SSAS.

2.11.24   The control measures that could be applied to a ship in port include:

  a   more detailed inspection of the ship, including searches - which could lead to the imposition of more stringent control measures;

  b   delaying the ship;

  c   detention of the ship;

  d   restrictions on operation – including unloading or loading and its movement within the port;

  e   expulsion from the port; and

  f   lesser administrative or corrective measures.

Notifications

2.11.25   When control measures are taken with respect to a ship, the ship's Administration and the RSO that issued the ship's ISSC or Interim ISSC should be notified without delay.

2.11.26   Under the Maritime Security Measures, Administrations are required to establish a contact point that can be available at any time to receive and act upon reports from Governments exercising control and compliance measures.

2.11.27   Refusing a ship the right to enter port, the detention of a ship or the expulsion of a ship from port has to be reported to the Consular representative of its flag State.

2.11.28   The control measures taken in respect of a ship under the Maritime Security Measures should also be reported to the Organization.

2.11.29   Control measures should only be imposed until the non-compliance which gave rise to them is rectified.

2.11.30   Every effort should be taken to avoid undue detention or delay. The Maritime Security Measures provide for compensation to be claimed for loss or damage if a ship is unduly delayed.

Immediate security threat

2.11.31   Denial of entry into port or expulsion from port should only be imposed if the duly authorized officer believes that the ship poses an immediate security threat and that there is no other appropriate means of removing the threat.

2.11.32   In such instances, other States whose ports the ship is known to be intending to visit, and any relevant coastal States, should be informed in confidence of the circumstances which led to the denial or expulsion.

2.11.33   The same procedure could be followed if a ship intending to enter port refuses to permit an inspection when notified by a duly authorized officer of the intention to take control measures.

Experience to date

2.11.34   The reports of Port State Control Memoranda of Understanding indicate that security-related deficiencies represent some 3 to 5% of the deficiencies found on SOLAS ships. Ships with security-related deficiencies are almost invariably found to have safety or other deficiencies.

2.11.35   Further guidance on aspects of control and compliance measures from the perspective of ship operators is in sub-section 4.10. A more detailed description of implementing control and compliance measures can be found in the Procedures for Port State Control booklet which is referenced on the IMO publications webpage at: www.imo.org

2.12   Ship Security Communications

Requirement for alert and identification systems

2.12.1   Under the Maritime Security Measures, all SOLAS ships have to have a ship security alert system (SSAS).

2.12.2   Under provisions elsewhere in the SOLAS Convention, the following SOLAS ships are required to be fitted with an Automatic Identification System (AIS):

     a   passenger ships irrespective of size;

     b   cargo ships of 300 gross tons and upwards engaged on international voyages;

     c   cargo ships of 500 gross tons and upwards *not* engaged on international voyages

2.12.3   Also under provision elsewhere in the SOLAS Convention, the following SOLAS ships engaged on international voyages have to be fitted with a long range identification and tracking (LRIT) system:

     a   passenger ships, including high speed craft;

     b   cargo ships, including high speed craft, of 300 gross tons and upwards,

     c   mobile offshore drilling units

Ship Security Alert Systems

2.12.4   A Ship Security Alert System (SSAS) transmits a covert alarm to one or more competent authorities ashore indicating that the security of the ship is under threat or has been compromised. Ship security alerts can be activated in the event of any serious security incident including acts of piracy and armed robbery against the ship.

2.12.5   Guidance on SSAS installation and operation on ships is in paragraphs 4.6.1 to 4.6.11. These details need not be included in SSPs but can be included in a separate document known to the master, SSO or other senior shipboard personnel selected by the company.

2.12.6   Administrations designate one or more competent authorities ashore to receive ship security alerts from their SOLAS ships. Any designated competent authority should be able to obtain a covert verification from the ship and alert the country's security forces responsible for initiating the security response to acts of violence against ships.

2.12.7   Administrations have to establish an effective means of communication between their competent authorities and the security force responsible for the response.

2.12.8   Many Administrations have designated CSOs and a selected Maritime Rescue Coordination Centre (MRCC), or equivalent agency, as their competent authorities. Protocols have to be in place to ensure immediate communication between CSOs receiving a ship security alert and the selected competent authority (which is the point of contact with the responding security force). CSOs are often in the best position to seek verification of alerts from their ships. Covert verification can be achieved by pre-arranged exchanges of messages.

2.12.9   Others Administrations have designated a MRCC as their sole competent authority for the receipt of ship security alerts. In such cases, the MRCC should establish procedures for verifying individual ship security alerts.

2.12.10   Unless directed by the Administration or security force, a competent authority who receives a ship security alert should not overtly acknowledge its receipt to the ship.

2.12.11   Administrations should provide guidance to competent authorities on the procedures to be followed on the:

      a   prioritization of ship security alerts;

      b   distinction between covert and overt alarms;

      c   receipt of false security alerts and distress/security double alerts; and

      d   testing ship security alert systems and associated communication procedures.

2.12.12   The IMO has requested that information be provided on the receipt of false security alerts and distress/security double alerts.

2.12.13   Administrations should ensure that ships that flying their flag test ship security systems and associated communication procedures on a regular basis. When doing so, it should be made clear that it is a TEST alert.

2.12.14   In consultation with their responding security forces, Administrations should develop protocols on notifying MRCCs in the vicinity of the ship, their Governments, and the Administrations or response organizations in adjacent countries, of the receipt of an alert.

2.12.15   Upon receiving notification of a security alert from a ship entitled to fly its flag, the Administration must immediately notify the State(s) in the vicinity of which the ship is presently operating. If a security alert is received from a ship that is not entitled to fly its flag, that Contracting Government must immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

Automatic identification systems

2.12.16   Regulation 19 of SOLAS Chapter V requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The requirement became effective for all ships by December 31, 2004.

2.12.17   Ships fitted with AIS are expected to maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information. A flag State may exempt ships from carrying AIS when ships will be taken permanently out of service within two years after the implementation date. Performance standards for AIS were adopted in 1998.

2.12.18   The regulation requires that AIS shall:

      a   provide information – including the ship's identity, type, position, course, speed, navigational status and other safety-related information – automatically to appropriately equipped shore stations, other ships and aircraft;

      b   receive automatically such information from similarly fitted ships;

      c   monitor and track ships; and

      d   exchange data with shore-based facilities.

2.12.19   AIS-generated ship data is not available on open source internet sites as it is considered to be detrimental to the safety and security of ships and port facilities and undermines the efforts of the IMO and its Member States to enhance the safety of navigation and security in the international maritime transport sector.

Pre-Arrival Notification

2.12.20   As explained in sub-section 2.11 on Control and Compliance Measures, a ship intending to enter a port of another Contracting Government may be required to provide the following information to responsible officials:

    a   confirmation of a valid ISSC and the name of its issuing authority;

    b   the Security level at which it is currently operating;

    c   the Security level at which it operated in the last 10 ports of call where it conducted a ship/port interface;

    d   any special or additional security measures that were taken in the last 10 ports of call where it conducted a ship/port interface e.g. Declarations of Security;

    e   confirmation that the appropriate ship security procedures were maintained during any ship-to-ship activity during the last 10 ports of call e.g. with ships that are not required to comply with the Maritime Security Measures or persons and goods rescued at sea;

    f   other practical security-related information, but not details of the SSP. Examples include:
- information contained in the Continuous Synopsis Record;
- the location of the ship at the time of reporting;
- the expected time of arrival;
- crew and passenger lists;
- general description of cargo being carried;
- person(s) responsible for appointing crew and other shipboard personnel;
- information on charter parties.

2.12.21   The Contracting Government may seek supplementary information as a condition of entry or, subsequent to entry, additional information to validate the data set provided. The request for supplementary information may not include details of the SSP.

2.12.22   Details of a ship's responsibilities in providing the above information are documented in paragraphs 4.6.13 to 4.6.15.

2.12.23   Experience to date indicates that Administrations have established standing requirements on:

    a   the information to be provided;

    b   the form on which information is to be provided; and

    c   the time period required for submission of pre-arrival information.

2.12.24   The IMO has developed the standard data set in this respect (refer to Appendix 4.6 – Standard Data Set of Security-related Pre-Arrival Information). Administrations are expected to advise shipping companies of these requirements (as their ships will not be requested for the information by duly authorized officers).

Long Range Identification and Tracking systems

2.12.25   Long Range Information and Tracking (LRIT) was developed at the IMO as a means of enhancing maritime security by providing ship identity and current location information in sufficient time for a Contracting Government to evaluate the security risk posed by a ship off its coast and to respond, if necessary. A robust international scheme for long-range identification and tracking of ships is an important and integral element of maritime security.

2.12.26   The LRIT regulation in the SOLAS Convention (refer to Chapter V, Regulation 19-1) entered into force on January 1, 2008, with all ships now required to be compliant with the exception of ships operating exclusively in coastal areas defined by its Administration and fitted with an AIS.

2.12.27   LRIT is a satellite-based tracking system designed to utilize existing shipboard equipment such as the Global Maritime Distress and Safety System (GMDSS) to track SOLAS-class vessels over 300 tonnes on international voyages. Four times daily and at six hour intervals, ships are required to transmit LRIT information, which is comprised of:

    a   the ship's identity;

    b   the ship's location (latitude and longitude); and

    c   the date and time of the position.

2.12.28   Unlike AIS, LRIT communication is addressed (i.e. it is a secure point-to-point transmission of information) rather than a broadcast.

2.12.29   While routine tracking is every six hours, the performance standards stipulate that onboard terminals must be capable of being remotely reconfigured to transmit LRIT information as frequently as every 15 minutes. Once communication has been established, the satellite terminal automatically responds to subsequent polling requests.

2.12.30   Each Administration must have a Data Centre (DC) to which its ships transmit. The DC is the repository of all of the Flag State's LRIT information and is connected to the wider International LRIT system via the International Data Exchange (IDE), through which all information is routed to other DCs. A Government not wishing to establish its own DC may utilize the services of another DC. Each Administration can associate itself with only one DC. The majority of Administrations contract their DC services to third-party service providers.

2.12.31   Data is collected by each Administration by means of its DC and shared with requesting Contracting Governments based on strict entitlements defined in the SOLAS regulation. In addition to establishing or joining a DC, each Government that has flag vessels must formally appoint an Application Service Provider to:

     a   conduct conformance tests on those ships;

     b   manage the associated communications between the ship, the Communications Service Provider and the DC; and

     c   issue ships with a Conformance Test Report.

2.12.32   A Contracting Government is entitled to request and receive LRIT data about ships:

     a   entitled to fly its own flag irrespective of where the ships are located;

     b   flying the flag of another Contracting Government that have indicated their intention to enter a port facility under the jurisdiction of the requesting Contracting Government; and

     c   flying the flag of another Contracting Government that are navigating within 1000 nautical miles of the coast of the requesting Contracting Government.

2.12.33   An Administration may at any time, in order to meet security or other concerns, decide not to provide LRIT information about its ships to another Contracting Government. In such a case, the Administration concerned must communicate its decision to the IMO which, in turn, is required to inform all Contracting Governments of the action. To date, no Administration has done so.

2.12.34   International agreement restricts data use to Contracting Governments and Search and Rescue (SAR) authorities. Contracting Governments can share within their own government the data that they receive in response to a request from another Contracting Government. However, data requested or received by a SAR Authority within a Contracting Government must only be used for SAR purposes.

2.12.35   As LRIT is a user pay system, all requesting Data Centres must pay DCs supplying information for the information that is received. Experience to date indicates that a regular LRIT position report typically costs the equivalent of US$0.25 US while a poll costs US$0.50 and a terminal reconfiguration US$3.00.

2.12.36   All requests for and receipts of LRIT information are logged in a journal maintained by the IDE. This journal is used for costing and billing, as well as for auditing purposes.

2.12.37   The International Mobile Satellite Organization (IMSO) provides oversight of the international LRIT system and conducts annual audits of each LRIT Data Centre.

2.13   Alternative Security Agreements

Introduction

2.13.1   Governments can conclude bilateral or multilateral Alternative Security Agreements (ASAs) for short international voyages on fixed routes between dedicated port facilities. These agreements allow the security measures and procedures applied to the port facilities and ships to differ from those required under the Maritime Security Measures.

2.13.2   Elsewhere in the SOLAS Convention, a short international voyage is defined in the context of life-saving appliances and arrangements as: "… an international voyage in the course of which a ship is not more than 200

miles from a port or place in which the passengers and crew could be placed in safety.   Neither distance between the last port of call in the country in which the voyage begins and the final port of destination nor the return voyage shall exceed 600 miles. The final port of destination is the last port of call in the scheduled voyage at which the ship commences its return voyage to the country in which the voyage began."

Application

2.13.3   The port facilities included in an ASA can only interface with ships operating on the fixed routes to which the ASA applies.

2.13.4   All ships operating on the fixed route between the port facilities covered by an ASA have to be covered by that ASA.

2.13.5   Third flag vessels can be covered by an ASA if their Administration ensures that their ships fully comply with the provisions in the ASA.

2.13.6   The ships covered by an ASA cannot conduct any ship-to-ship activity with a ship not covered by the ASA or ship/port interfaces at any other port facility.

Procedure

2.13.7   A combined port facility and ship security assessment should be undertaken by the national authorities and other relevant government organizations (e.g. Customs and Immigration Services) of the States involved.

2.13.8   The combined security assessment should be based on a shared understanding of the security risks likely to be associated with the port facilities, ships and voyages to be covered by the proposed agreement. It should cover all ship/port interfaces at the port facilities and any ship-to-ship activities to be undertaken between the ships.

2.13.9   When undertaking such a combined security assessment, National Authorities should consult the relevant authorities in any country likely to be affected by the operation of the proposed agreement.

2.13.10   The combined assessment should identify the security measures and procedures appropriate at the port facilities and to the ships, involved. All parties to the Agreement should approve the combined security assessment and the resulting security measures and procedures.

2.13.11   The respective National Authorities should then take the necessary actions to ensure that the required security measures and procedures are applied and maintained at the port facilities and on the ships for the duration of the Agreement.

2.13.12   The security procedures should ensure that the required control measures applying to embarking passengers and vehicles are carried out at the port facility prior to the loading of a ship when the ship, such as a Ro-Ro ferry, has a short turn-round time.

2.13.13   National Authorities concluding such Agreements are required to notify the IMO by accessing the Alternative Security Agreement screen in GISIS (refer to paragraph 2.19.2) at http://gisis.imo.org/ and providing the following information:

      a   Ships and port facilities covered by the agreement;
      b   Name of arrangement;
      c   Fixed route covered by the arrangement;
      d   Information on consultation with other governments;
      e   Date of entry into force of arrangement;
      f   Periodicity of review of arrangement; and
      g   Has security arrangement been withdrawn?

2.13.14   Further guidance on Alternative Security Agreements is in sub-sections 3.2 and 4.2.

Review

2.13.15   The operation of an Alternative Security Agreement should be continually monitored and reviewed in the light of experience. A review should take place if there is any significant security threat or incident involving the port facilities or ships covered by the Agreement.

2.13.16   Under the Maritime Security Measures, Alternative Security Agreements have to be reviewed every five years.

Experience to date

2.13.17   Alternative Security Agreements have covered such aspects of international ferry services as:
- a   Ship security alerts;
- b   Security personnel identification and screening;
- c   Reciprocal recognition of SSP approvals;
- d   Acceptance of minor differences in regulatory requirements; and
- e   Alternative security requirements to those in the Maritime Security Measures.

2.14   Equivalent Security Arrangements

2.14.1   National authorities can allow port facilities, groups of port facilities and ships to implement other security measures equivalent to those in the Maritime Security Measures. Such measures have to be at least as effective as those prescribed in the Maritime Security Measures. Few national authorities have allowed equivalent security arrangements.

2.14.2   Designated Authorities can allow a port facility or a group of port facilities to implement security measures or procedures equivalent to those in the Maritime Security Measures without having to appoint a PFSO or submit a PFSP. However, these Equivalent Security Arrangements (ESAs) are allowed only under limited circumstances, applying to port facilities with more than occasional use by SOLAS ships but without frequent services or involving special operations (e.g. berths used by SOLAS ships at naval facilities with military security measures and procedures).

2.14.3   As with port facilities used only occasionally by SOLAS ships, the equivalent security arrangements allowed by Designated Authorities should identify a person ashore with responsibility for shore-side security including the completion of a DOS.

2.14.4   ESAs should not be used as a stop gap allowing port facilities frequently used by SOLAS ships to delay or avoid full implementation of the Maritime Security Measures.

2.14.5   Similarly, ESAs should not allow SOLAS ships to avoid full compliance with the requirements of the Maritime Security Measures.

2.14.6   National authorities concluding such arrangements are required to notify the IMO by accessing the Equivalent Security Arrangement for Ships or for Port Facilities screen in GISIS at http://gisis.imo.org/ and providing the following information:
- a   Name of Ships or Port Facilities
- b   Name of the Arrangement; and
- c   Description of the Arrangement.

2.14.7   A limited number of ESAs have been reported to the IMO. A number apply to port facilities occasionally used by SOLAS ships. For ships, some apply to ships operating regional shipping services while others appear to apply to ships trading internationally.

2.14.8   The limited particulars of individual ESAs does not allow any useful assessment of experiences to date.

2.15   Enforcement Actions

Introduction

2.15.1   Governments are ultimately responsible for ensuring that their port facilities and SOLAS ships fully comply with the Maritime Security Measures.

2.15.2   For SOLAS ships, failure to comply with the Maritime Security Measures could lead to Governments applying control measures against non-compliant ships. The application of control measures in this way can ultimately have significant implications for all ships flying the State's flag and are best avoided by ensuring compliance with the Maritime Security Measures.

2.15.3   Security inspections of their port facilities and SOLAS ships by national authorities can result in enforcement action to ensure correction of any identified security deficiencies and prevent such deficiencies recurring in future.

2.15.4   The enforcements actions following the identification of security deficiencies will depend on:

   a   whether the deficiencies prevent the port facility or SOLAS ship from continuing to operate at Security levels 1 to 3;

   b   whether the deficiencies compromise the ability of the port facility or SOLAS ship from continuing to operate at Security levels 1 to 3;

   c   the extent of the sanctions available to the national authorities under their legislation.

2.15.5   Whatever the ultimate sanctions available to a national authority are, Governments should take a stepped approach when seeking to ensure that the port facility or ship corrects an identified deficiency which does not prevent the port facility or ship from continuing to operate at security levels 1 to 3. A more robust approach may have to be taken if a port facility or ship has a security deficiency which compromises its ability to operate at security levels 1 to 3.

Stepped approach

2.15.6   A stepped approach follows distinct steps:

   a   advice to the port facility or ship on correcting the deficiency;

   b   further persuasion of the port facility or ship on the need to correct the deficiency;

   c   formal notification of the requirement to correct the deficiency;

   d   commencement of proceedings to impose sanctions for the failure to correct the deficiency;

   e   the imposition of sanctions for failing to correct the deficiency.

2.15.7   An example of a stepped approach is shown below:

Type of Enforcement Action	Seriousness of Contravention	Impact on Operator	Legal basis for Action
Counselling	Minor	Low	None required
Notice of Non-compliance	Minor	Low	None required
Compliance Agreement (in lieu of penalty)	Moderate	Low to Medium	Required
Fine	Moderate	Medium	Required
Suspension or restriction of activities	Significant	Medium to High	Required
Withdrawal of Certificate or Statement of Compliance	Significant	Medium to High	Required
Imposition of Penalties	Significant	High	Required

2.15.8   The procedures followed at each step should be taken in the knowledge that ultimately sanctions may have to be imposed. The maintenance of evidence of the deficiency and of records of the actions taken at each stage could be essential if proceedings are taken imposing sanctions and if they are to be upheld in any subsequent appeal proceedings

Counselling

2.15.9   Once a deficiency is identified details should be recorded and evidence collected and protected. The deficiency should immediately be discussed with the PFSO or SSO to establish what action is needed to correct the deficiency. Advice could be offered on the appropriate actions to take.

2.15.10   Temporary alternative security procedures or measures could be agreed with the port facility or ship which should be applied until the original deficiency is corrected. Records should be kept of all discussions with the PFSO or SSO. A period should be agreed in which the deficiency should be corrected and a further inspection undertaken.

2.15.11   If it is established that the deficiency has not been corrected within the agreed time, efforts should be made to persuade the PFSO or SSO of the need to correct the deficiency and to maintain the agreed temporary alternative security procedures or measures. At this stage, the national authority may seek to involve the port facility operator or, in the case of ships, the CSO. Records should be kept of any discussion and the PFSO or SSO should be advised in writing of the deficiency and the action required to correct the deficiency.

Formal notification

2.15.12   If informal advice and persuasion has not secured correction of the deficiency, or if the deficiency is serious or recurring, the PFSO, Master or SSO should receive a formal notification in writing describing the deficiency, the action needed to correct it, and the PFSO's, Master's or SSO's responsibility to remedy the deficiency. Emphasis could be placed on the possible security and safety implication of the continued deficiency for the ship and those using the facility. A sample of such a notice is shown in Appendix 2.9 – Sample of a Notice of Non-Compliance, for a SOLAS ship; the notice for a port facility would be similar.

2.15.13   The formal notification should set a period of time within which the deficiency should be corrected. Also, it should advise that failure to correct the discrepancy within that period could lead to the commencement of formal proceedings to achieve compliance which, in turn, could lead to sanctions being imposed on the port facility or ship.   The formal notification should be issued to the senior management of the port facility or shipping company rather than the PFSO/SSO/CSO.

2.15.14   Once again it is important to record all contacts and to retain and protect correspondence and evidence relating to the deficiency.

Serious security deficiencies

2.15.15   Serious security deficiencies are those which compromise the ability of the port facility or SOLAS ship to continue to operate at Security levels 1 to 3.

2.15.16   Immediate action may need to be taken to secure correction of such deficiencies and, initially, the inspector should discuss with the PFSO, master or SSO alternative security measures and procedures of equal effect which could be put in place to allow the facility or ship to operate at Security levels 1 to 3. If such alternatives are identified and there is no immediate security risk the port facility or ship should be given reasonable time to introduce them.

Restriction or suspension of activities

2.15.17   If alternatives cannot be found or applied within a reasonable time frame, or if agreed alternative security procedures or measures have not been put in place, the national authority could, in the most serious cases, have the authority to be able to restrict or suspend specified activities at a port facility or on a ship.

2.15.18   A restriction notice could limit the activities that could be undertaken at the port facility or on the ship until action has been taken to correct the serious security deficiency.

2.15.19   When an immediate security risk linked to a specific activity has been identified, a suspension notice could stop the activity been undertaken by the port facility or ship pending correction of the serious security deficiency.

2.15.20   A restriction or suspension notice could be lifted when the national authorities consider:
   a   the serious deficiency has been corrected, or
   b   agreed security measures or procedures of equal effect are in place and operating effectively.

Suspension or withdrawal of an approved PFSP or SSP

2.15.21   There could be circumstances when cumulative security failings at a port facility or on a ship could lead to the:

a   suspension or withdrawal of the approved PFSP, and Statement or Compliance if issued; or

b   suspension or withdrawal of the approved SSP and ISSC.

2.15.22   National authorities may require completion of a PFSA and submission of an amended PFSP before reinstating a PSFP which has been suspended or withdrawn.

2.15.23   Similarly a new SSA may have to be undertaken and an amended SSP submitted before a suspended or withdrawn SSP can be reinstated and initiation of the procedures leading the re-issue of an ISSC.

Imposition of penalties

2.15.24   In the occasional situation that none of the preceding steps has resulted in correction of the deficiency, the national authority may commence proceedings to seek sanctions against the port facility or ship operator.   The procedures should be clearly stated in national legislation and are likely to include the right to appeal against the imposition of sanctions.

2.15.25   The proceedings could involve hearings before an administrative or judicial tribunal where the national authority is required to explain and, if necessary, defend the actions that it has taken to seek correction of the deficiency.   The documentary evidence of the actions taken and of the deficiency could be essential to the success of the national authority's case.

2.15.26   The sanctions that can be imposed on a port facility or ship for failure to correct an identified deficiency should, again, be specified in national legislation.   The authority to impose sanctions may rest with a senior official within the national authority or judicial body.   Sanctions could include administrative, civil and criminal penalties. The national authority may be required to sustain its case through any appeal procedures that might follow the imposition of sanctions. The sanctions should be effective, proportional and persuasive.

2.16   Training of government officials with security responsibilities

Introduction

2.16.1   Government officials undertake an extensive range of responsibilities under the Maritime Security Measures relating to all aspects of port facility and ship security. Ensuring individual officials have the knowledge and competencies needed to undertake their responsibilities can make a significant contribution to the effective implementation of the Maritime Security Measures.

2.16.2   The following paragraphs provide guidance on the competencies that Government officials could have to allow them to successfully undertake their responsibilities relating to the implementation or oversight of the Maritime Security Measures.

Duties of officials

2.16.3   The duties of officials working in Designated Authorities could include:

a   advising on, and overseeing, the implementation of the Maritime Security Measures to port facilities;

b   drafting and implementing national legislation and regulations implementing the Maritime Security Measures for port facilities;

c   consulting ports and related industries on security issues;

d   communicating the applicable Security level;

e   determining which port facilities used by SOLAS ships have to appoint a PFSO and prepare a PFSP;

f   appointing a person ashore with responsibility for shore-side security at port facilities occasionally used by SOLAS ships to liaise with SOLAS ships using that facility;

g   authorizing RSOs to undertake port facility related tasks for the Designated Authority and subsequently monitoring their activities and outputs;

h   advising on security threats;

i   undertaking, reviewing and approving PFSAs including those undertaken by RSOs;

j   determining policy on Declarations of Security;

k   determining the requirements for port facilities to report security incidents;

l   determining the security records to be kept by port facilities and the duration of retention;

m   advising on the preparation and content of PFSPs;

n   reviewing and approving PFSPs and determining the types of amendments to an approved plan that have to be submitted for approval;

o   undertaking inspections and verification relating to the issue and endorsement of Statements of Compliance, and

p   undertaking inspections of port facilities to assess their compliance with the Maritime Security Measures.

2.16.4   The duties of officials working in Administrations could include:

a   advising on and overseeing the implementation of the Maritime Security Measures for ships;

b   drafting and implementing national legislation and regulations implementing the Maritime Security Measures for ships;

c   consulting the shipping and related industries on security issues;

d   communicating, the applicable Security level;

e   authorizing RSOs to undertake delegated responsibilities for the Administration and subsequently monitoring their activities and outputs;

f   advising on security threats;

g   advising on the preparation of SSAs;

h   determining policy on Declarations of Security;

i   determining the requirements for reports of security incidents from ship;

j   determining the security records to be kept by ships and the duration of retention;

k   advising on the preparation and content of SSPs;

l   assessing and approving SSPs and determining the type of amendments to an approved plan that have to be submitted for approval;

m   undertaking inspections and verification relating to the issue and endorsement of International Ship Security Certificates;

n   issuing Interim International Ship Security Certificates:

o   exercising control and compliance measures under the Maritime Security Measures to foreign-flagged vessels using, or intending to use, their ports;

p   undertaking inspections of their SOLAS ships to assess their compliance with the Maritime Security Measures;

q   advising on the security procedures and measures appropriate for non-SOLAS vessels;

r   issuing Certificates of proficiency to shipboard personnel under the STCW Convention and Code (refer to paragraphs 2.9.1 to 2.9.11 and sub-section 4.5).

Training requirements

2.16.5   Given the range of duties that Government officials can exercise under the Maritime Security Measures, their training should impart an appropriate level of knowledge of:

a   the drafting and implementing national legislation including regulations;

b   the requirements of the Maritime Security Measures relating to port facilities and ships;

c   the supervision of RSOs authorized to undertake duties for national authorities;

d   the security threats that could be experienced at port facilities and on ships;

e   risk assessments of security incidents;

f	the security measures and procedures appropriate to mitigate security threats that could occur at port facilities and ships;
g	the completion and assessment of PFSAs;
h	the preparation and content of SSAs;
i	the preparation, content, submission and approval of PFSPs and SSPs;
j	the content, submission and approval of amendments to approved PFSPs and SSPs;
k	the undertaking of inspections or verifications associated with the issue and endorsement of Statements of Compliance of a Port Facility;
l	the undertaking of inspections or verifications associated with the issue and endorsement of International Ship Security Certificates;
m	the undertaking of inspections and assessments relating to the issue of Interim International Ship Security Certificates;
n	the exercise of control and compliance measures in respect of foreign-flagged vessels to assess their compliance with the requirements of the Maritime Security Measures;
o	the undertaking of security inspections of port facilities and SOLAS ships to assess their compliance with national security requirements – including the collection and protection of evidence relating to identified security deficiencies where enforcement action may be required.

2.16.6   For a national authority to be confident that its inspectors are adequately qualified to carry out their delegated responsibilities, it is recommended that the authority have an approved training curriculum. Under such a scenario, the training may be delivered by external training organizations according to specifications determined by the national authority. The basic or core training elements, the details of which are shown as a sample curriculum in Appendix 2.10 – Sample of a Core Training Curriculum for Officials in National Authorities, could include:

a	Knowledge of the national authority's legislative framework
b	Knowledge of the international maritime security framework;
c	Knowledge of the maritime industry over which the authority has jurisdiction;
d	The responsibilities of the national authority specified in the Maritime Security Measures;
e	The responsibilities delegated to inspectors (attending the course);
f	Code of Conduct
g	Description of the authority's regulatory oversight program;
h	Procedures for preparing, conducting and reporting the results of verifications;
i	Procedures for handling cases of non-compliance;
j	Procedures for observing or participating in exercises;
k	Procedures for issuing, renewing, suspending and withdrawing certificates and other forms of authorization; and
l	Procedures for conducting awareness and education activities with industry and labour associations, port security committees and the public.

2.16.7   Experience to date indicates that:

a	for maximum effect and to facilitate practical sessions and participant involvement in discussion, the course size should be in the 6-12 course participants range;
b	Complementary to the above and as an integral part of the basic training requirements, workshops could be held on report writing, presentations, interviews and consultations; and
c	In the spirit of continuous learning, as the qualified personnel become more experienced, they should have access to more advanced training in specialized areas such as methodologies for conducting threat and risk assessments, techniques for investigating serious contraventions of regulatory requirements; and participation in emergency response and preparedness exercises.

Code of Conduct

2.16.8   The IMO issued a Code of Good Practice for Port State Control Officers in 2007 and invited its member Governments and regional port state control regimes to bring the Code to the attention of officials exercising port and coastal State actions. The 28-point Code is based on the following three main principles:

     a   Integrity – the state of moral soundness, honesty and freedom from corrupting influences or motives;

     b   Professionalism – applying accepted professional standards of conduct and technical knowledge;

     c   Transparency – implying openness and accountability.

2.16.9   The Code may be accessed at the IMO's internet site for its Circulars: http://docs.imo.org/Category.aspx?cid=538 or at the internet sites of regional port state control regimes.

2.16.10   Experience to date indicates that some national authorities have adapted the Code for their government officials and incorporated it into their training curriculum and oversight manuals as a code of conduct.

Identification Documents

2.16.11   Government officials are entitled as part of their duties to enter port facilities or board ships and as such should carry appropriate identification documents issued by the Government. Identification documents should include a photograph of the holder of the document. They should also include the name of the holder or have a unique identification number. If the identity document is in a language other than English, French or Spanish a translation into one of those languages should be provided.

2.16.12   Government officials should present their identification document when requested to do so at access points to port facilities and when boarding a ship.

2.16.13   Port facility and ship security personnel should be able to verify the authenticity of identity documents issued to Government officials and Governments should establish procedures, and provide contact details, to facilitate such validation.

2.16.14   Emergency response services and pilots should also carry appropriate identification documents and present them when boarding a vessel. The authenticity of such identification documents should be capable of being verified.

2.16.15   Only the person in charge of an emergency response team need present an identification document when accessing a port facility or boarding a ship and should inform the relevant security personnel of the number of emergency response personnel entering or boarding.

2.16.16   Government officials who are properly identified and acting in the course of their duties, emergency response personnel and pilots should not be required to surrender their identity documents when entering a port facility or boarding a ship. The issue of visitor identification documents by a port facility or a ship may not be appropriate when Government officials, emergency response personnel or pilots have produced an identity document which can be verified.

2.16.17   Government officials should not be subject to search by port facility or ship security personnel. Any search requirement in an approved security plan could be waived for emergency response personnel responding to an emergency or for a pilot boarding a ship once their identity has been verified.

2.16.18   Port facility security officers should assist ship security officers verify the identification of Government officials, emergency response personnel or pilots intending to board a ship.

2.17   National Oversight

Introduction

2.17.1   Under the Maritime Security Measures, Governments have the responsibility to assess the continuing effectiveness of the security measures and procedures required of their port facilities, shipping companies and ships and the RSOs authorized to act on their behalf.   Through control and compliance measures, Governments can also assess the compliance of foreign flagged ships using, or intending to use, their ports.

2.17.2   An effective oversight program should include continuous monitoring and evaluation of the Government's own performance in the implementation, application and operation of its specific security responsibilities under the Maritime Security Measures.

2.17.3   A national oversight program should allow Governments to determine the extent to which:

<table>
<tr><td>a</td><td>it has met all its obligations under the Maritime Security Measures;</td></tr>
<tr><td>b</td><td>appropriate advice and guidance has been offered to their port facility operators, shipping companies, ships and RSOs;</td></tr>
<tr><td>c</td><td>their port facility operators, shipping companies, ships and RSOs understand and meet their obligations under the Maritime Security Measures;</td></tr>
<tr><td>d</td><td>their port facilities implement the security measures and procedures in their PFSPs;</td></tr>
<tr><td>e</td><td>their SOLAS ships implement the security measures and procedures in their SSPs;</td></tr>
<tr><td>f</td><td>foreign-flagged vessels using their ports comply with the Maritime Security Measures;</td></tr>
<tr><td>g</td><td>inspections, verifications, audits, reviews and control measures promptly identify non-conformities;</td></tr>
<tr><td>h</td><td>immediate action is taken to correct non-conformities;</td></tr>
<tr><td>i</td><td>their officials undertaking inspections, verifications, reviews and control measures to assess compliance with the Maritime Security Measures have the required training and conduct themselves in a professional manner.</td></tr>
</table>

2.17.4   Although not mandatory, a set of governing principles, such as the one shown below, may influence how a national authority intends to implement its oversight program:

<table>
<tr><td>a</td><td>*Transparency,* by officials being as open as legislation and confidentiality requirements permit;</td></tr>
<tr><td>b</td><td>*Fairness,* by dealing with non-compliance through actions that are authorized, impartial and appropriate to the risk imposed by the non-compliance while ensuring that there is access to appeal procedures;</td></tr>
<tr><td>c</td><td>*Timeliness*, by making decisions in a timely manner;</td></tr>
<tr><td>d</td><td>*Consistency*, by interpreting, administering and enforcing legislation in a consistent manner;</td></tr>
<tr><td>e</td><td>*Confidentiality*, by applying all appropriate measures to protect confidentiality or sensitive information.</td></tr>
</table>

Seafarer Access Considerations

2.17.5   The 2002 SOLAS Conference that adopted the Maritime Security Measures and associated Conference resolutions was aware of the potential for the fundamental human rights of seafarers to be adversely affected by the imposition of a security regime on international shipping. It was recognized that seafarers would have the primary duties and responsibilities for implementing the security regime for ships. At the same time, there was concern that the emphasis on port facility security could result in ships and seafarers being viewed as a potential threat to security rather than as partners in the effective implementation of the security regime.

2.17.6   One of the resolutions adopted at the 2002 Diplomatic Conference urged Contracting Governments to take the need to afford special protection to seafarers and the critical importance of shore leave into account when implementing the provisions of the Maritime Security Measures.

2.17.7   In this regard, it was recognized that:

<table>
<tr><td>a</td><td>there may be conflicts between security and human rights as well as between security and the efficient movement of ships and cargos in international trade (that is essential to the global economy);</td></tr>
<tr><td>b</td><td>there should be a proper balance between the needs of security, the protection of the human rights of seafarers and port workers, and the requirement to maintain the safety, security and working efficiency of ships by allowing access to ship support services (e.g. loading stores, repair and maintenance of essential equipment, and other vital activities that are appropriately undertaken while moored at port facilities);</td></tr>
<tr><td>c</td><td>the ISPS Code must not be interpreted in a manner that is inconsistent with existing international instruments protecting the rights and freedoms of maritime and port workers; and</td></tr>
<tr><td>d</td><td>in approving port facility security plans, Contracting Governments should be aware of the need for seafarer's shore leave and access to shore-based welfare facilities and medical care.</td></tr>
</table>

2.17.8   The IMO considers that an essential part of national oversight activities is to verify that PFSPs contain provisions to facilitate:

<table>
<tr><td>a</td><td>shore leave by seafarers;</td></tr>
</table>

     b   shore access by ships' crews for operational and safety reasons;

     c   the access of legitimate visitors – including those undertaking maintenance or repairs on the ship and representatives of welfare organizations - to and from ships.

2.17.9   National authorities should ensure that:

     a   arrangements have been put in place to monitor the effective implementation of such provisions;

     b   there are no unbiased and non-discriminatory practices in allowing access to shore i.e. they are irrespective of ships' flags and the nationalities of individual crew members;

     c   neither seafarers nor their legitimate visitors should have to pay for the implementation of such provisions;

     d   all port facility security personnel are fully aware of the necessity to provide an adequate protection of seafarers' rights and of the humanitarian significance of shore leave.

2.17.10   Contracting Governments and representative organizations of seafarers and ship-owners are encouraged to report to the IMO any instances where the human element has been adversely impacted by the implementation of the provisions of the Maritime Security Measures. They are requested to bring instances of unfair and selective practices in providing shore leave and access to the shore-based facilities in foreign ports to the attention of the IMO's Maritime Safety and Facilitation Committees.

Port Facility Inspections

2.17.11   The frequency of port facility inspections should be determined by the Designated Authority. Inspections can be programmed and arranged in advance or they can be unannounced. Inspections can be undertaken in connection with:

     a   initial, intermediate and renewal verification of the port facility's Statement of Compliance;

     b   following up a report of a security incident, and

     c   assessments of the port facility's compliance with the Maritime Security Measures.

2.17.12   The Designated Authority can undertake covert test of the security measures and procedures at their port facilities.

2.17.13   Those undertaking inspections for the Designated Authority should have the power to enter port facilities and inspect all or, if appropriate, a sample of the facility's security measures, procedures, documentation and records. Areas for inspection could include:

     a   access control including to restricted areas;

     b   handling of cargo;

     c   delivery of ships' stores and bunkers;

     d   monitoring the port facility;

     e   handling threats, breaches of security and security incidents;

     f   security communications;

     g   audits and amendments;

     h   procedures for shore leave and visitors to the ship;

     i   procedures for ship-to-shore interface activities;

     j   evacuation procedures; and

     k   protection of sensitive security information, e.g. the security plan.

2.17.14   Appendix 2.11 – Sample of a Port Facility Security Inspection Report Form, provides a template for reporting on the results of inspections. It provides examples of questions that could be asked, or issues pursued, when undertaking an inspection as well as including questions that could be asked on the qualifications of:

     a   port facility security officers;

     b   personnel with security responsibilities; and

     c   personnel without security responsibilities.

2.17.15   Those undertaking inspections should record:

     a   the security procedures and measures inspected;

b	their observations on the security procedures and measures;
c	the identification of any deficiencies;
d	the action(s) required of the port facility to correct any identified deficiencies, and
e	the action to be taken by the Inspector or the Designated Authority.

2.17.16   The identification of deficiencies may lead to enforcement action by the Designated Authority (refer to subsection 2.15).

2.18   Additional security related instruments and guidance issued by the IMO

Introduction

2.18.1   The following paragraphs refer to the security instruments and guidance issued by the IMO on:

a	Non-SOLAS vessels;
b	port security;
c	the Suppression of Unlawful Acts (SUA) Convention;
d	offshore activities; and
e	specific security issues, including:

- piracy and armed robbery;
- drug smuggling;
- stowaways;
- illegal migration; and
- the security of dangerous goods.

2.18.2   This guidance does not relate specifically to the Maritime Security Measures and Governments retain complete discretion as to the extent they consider the guidance should be reflected, if at all, in PFSAs, PFSPs, SSAs and SSPs prepared under the Maritime Security Measures.

Non-SOLAS Vessels

2.18.3   The Maritime Security Measures do not apply to non-SOLAS ships. However, Governments were specifically encouraged by the IMO to establish appropriate measures to enhance the security of ships and port facilities not covered by the Maritime Security Measures, including mobile offshore drilling units on location, and fixed and floating platforms not covered by the Maritime Security Measures.

2.18.4   Governments have complete discretion as to the action they take in respect of their ships and port facilities that are not covered by the Maritime Security Measures. As a result, several Governments have extended the Maritime Security Measures, in whole or part, to domestic passenger shipping services and the port facilities they use; some of these envisage extension to domestic cargo services if a risk assessment establishes the need.

2.18.5   Some Governments have applied security requirements to all their ships and port facilities, including fishing vessels and recreational craft also covering, fishing ports and marinas. Others have focused on harbour craft or other craft that engage in ship-to-ship activities with ships covered by the Maritime Security Measures.

2.18.6   The action taken by Governments in respect of non-SOLAS vessels should rest on an objective assessment of the security risk that such vessels can pose for themselves or through their interaction with ships covered by the Maritime Security Measures.

2.18.7   The IMO has developed a risk assessment and management tool (refer to Section 5) to allow government officials responsible for administering non-SOLAS vessels and non-SOLAS vessel operators to consider:

a	the security risks associated with each category of vessel;
b	the security measures and procedures operators of non-SOLAS vessels could take to mitigate the identified risks.

2.18.8   Some national authorities offer guidance to non-SOLAS vessel operators aimed at:

a	enhancing security awareness;

> b   fostering links between the operators of such vessels and the Government's maritime security services;
>
> c   establishing procedures to facilitate reporting of suspicious activities and other security concerns to the Government's maritime security services.

2.18.9   As part of enhancing security awareness, national authorities may wish to develop security policies and procedures to ensure that all operators and crew of non-SOLAS vessels are aware of the basic security measures applying to their vessel. In appropriate circumstances, passengers could also be advised on the basic security measures applying to the vessel on which they are travelling.

2.18.10   National Authorities may recommend basic security familiarization training for all crew members of non-SOLAS vessels to enable them to respond to security threats. In high risk areas, such training should allow for assessment of their response capability. The proficiency training provided for pleasure craft owners and operators could also encompass security awareness familiarization.

2.18.11   Any guidance to non-SOLAS vessel operators should cover the likely need to agree a Declaration of Security when undertaking ship-to-ship activities with a SOLAS ship or when entering a port facility where the Maritime Security Measures apply.

2.18.12   To enhance the control exercised by national authorities controlling port arrivals and departures, non-SOLAS vessels engaged on international voyages could be required to provide arrival and departure information including:

> a   particulars of the vessel;
>
> b   date/time of arrival or departure;
>
> c   position of the vessel off, or in, the port;
>
> d   particulars of Master/owner/shipping line/agent;
>
> e   purpose of call;
>
> f   cargo on board;
>
> g   crew and passenger lists;
>
> h   emergency contact information.

2.18.13   Similarly pleasure craft and other non-SOLAS vessels could be requested to provide voyage information including time of departure, destination and planned route. This information can assist the relevant authorities with their traffic monitoring activities and facilitate search and rescue operations if the vessel is in distress.

2.18.14   Difficulties can arise and delays occur when Government organizations are unable to establish the identity of non-SOLAS vessels engaged on international voyages.   The requirement for a unique IMO identification number does not apply to:

> a   vessels solely engaged in fishing;
>
> b   vessels without mechanical means of propulsion;
>
> c   pleasure yachts;
>
> d   vessels on special service e.g. light vessels and SAR vessels;
>
> e   hopper barges;
>
> f   hydrofoils and air cushion vehicles;
>
> g   floating docks and similar structures;
>
> h   wooden vessels;
>
> i   seagoing merchant vessels of less than 100gt; and
>
> j   all cargo vessels of less than 300gt.

2.18.15   In such cases, Administrations could consider establishing procedures to allow the identity of their non-SOLAS vessels to be confirmed by other Governments without significant delay. This form of liaison is well developed in many regional counter-narcotics agreements. Governments could also consider recommending to non-SOLAS vessel operators that that the fitting of automated tracking equipment on their vessels would result in several benefits including:

> a   enhanced safety and security;
>
> b   rapid emergency response to accidents and casualties;

c   enhanced SAR capabilities; and
    d   enhanced control of smuggling and illegal migration.

Port Security

2.18.16   The IMO approved the guidance on wider port security provided in the ILO/IMO Code of Practice on Port Security. This guidance relates to port areas which include port facilities as defined in, and designated under, Maritime Security Measures.

2.18.17   The guidance in the Code of Practice suggests that Governments should:
    a   develop a port security strategy;
    b   identify port areas required to appoint a port security committee and appoint a Port Security Officer (PSO);
    c   prepare and approve, port security assessments (PSAs); and
    d   prepare and approve port security plans (PSPs).

2.18.18   PSAs and PSPs should be approved by the Designated Authority responsible for port facility security under the Maritime Security Measures.

2.18.19   The provisions in a PSP should not conflict or override with any security measures and procedures contained in the approved PFSPs of the port facilities located within the port area.

2.18.20   Several European Governments have enacted legislation establishing a Port Security Authority (PSA) for some of their port areas. The PSA appoints a PSO and is required to submit a Port Security Risk Assessment and Port Security Plan to the Designated Authority for approval.

SUA Convention

2.18.21   Most Contracting Governments that have adopted the SOLAS Convention have also ratified the Organization's Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) and the related Protocol. The original 1988 SUA treaties provided the legal basis for action to be taken against persons committing unlawful acts against ships, including the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board which are likely to destroy or damage the ship. Contracting Governments are obliged either to extradite or prosecute alleged offenders.

2.18.22   Two new protocols to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 and its Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, 1988 (the SUA Treaties) were adopted on 14 October 2005. The two new Protocols expand the scope of the original Convention and protocol to address terrorism by including a substantial broadening of the range of offences and introducing boarding provisions for suspect vessels.

2.18.23   The revision took into account developments in the UN system relating to countering terrorism. The relevant UN Security Council resolutions and other instruments, including the International Convention for the Suppression of Terrorist Bombings (1997), and the International Convention for the Suppression of the Financing of Terrorism (1999) are directly linked to the new SUA protocol.

2.18.24   Drafted to criminalize the use of a ship "when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act", these new instruments represent another significant contribution to the international framework to combat terrorism.

2.18.25   The 2005 amendments to the SUA Convention and the related Protocol entered into force on 28 July 2010.

Offshore activities

2.18.26   Although the Maritime Security Measures do not extend to offshore activities or installations located on a State's Continental Shelf, Governments with significant offshore activities, particularly those linked to exploiting oil or gas reserves, have developed specific security requirements applying to ships engaged in offshore activities, to mobile offshore drilling units on location and to fixed and floating platforms. When foreign flagged ships are

engaged in offshore supply or support activities on a State's Continental Shelf, they can be covered by both the requirements of the Maritime Security Measures and any additional security requirements set by the coastal State.

2.18.27   Under their National law a limited number of Governments have defined fixed platforms located on their Continental Shelf as port facilities requiring appointment of a PFSO and preparation of a PFSP. Such provisions can extend to include Floating Production Storage (FPSO) vessels associated with oil and gas exploitation.

Specific security issues

2.18.28   It is for Governments to determine the extent to which the guidance issued by the Organization on the following is reflected when undertaking PFSAs and SSAs and in PFSPs and SSPs:

    a   piracy and armed robbery;

    b   drug smuggling;

    c   stowaways;

    d   illegal migration; and

    e   the security of dangerous goods

2.19   Information to the IMO

Introduction

2.19.1   Through their national authorities, Governments are required to provide the IMO with information on their national contact points and details on other aspects of their responsibilities including legislation, RSOs, security agreements and arrangements, designated port facilities and PFSP approvals.

Global Integrated Shipping Information System

2.19.2   The IMO Secretariat launched the Global Integrated Shipping Information System (GISIS) in 2005 to allow:

    a   direct reporting by Member States in compliance with existing requirements; and

    b   access to data compiled by the Secretariat.

2.19.3   The GISIS website which may be accessed at: http://gisis.imo.org

2.19.4   GISIS has two login-options: a member login and a public user login. The former is limited to IMO Member States and organizations with consultative or observer status at IMO whereas the public user login has read-only access to a limited amount of the information provided in GISIS.

National contact points

2.19.5   Effective international application of the Maritime Security Measures is dependent on the maintenance of strong communication links and liaison between port facility and ship operators on the one hand, and the National Contact Points to which they can express security concerns and from which they can seek security advice on the other.

2.19.6   To this end, Governments are required to provide the IMO with up-to-date information on the points of contact for their national authorities. The template designed for this purpose is included as Appendix 2.12 – Details of National Authority Contact Points. A separate form is to be completed for each of the following national contact points:

    a   National authority responsible for ship security;

    b   National authority responsible for port facility security;

    c   Recipient of ship security alerts;

    d   Recipient of security-related communications from other Governments;

    e   Recipient of security concerns from ships and requests for advice and assistance on ship-related security incidents and issues;

    f   Those who have been designated to be available at all times to receive and act upon reports from Governments exercising control and compliance measures.

2.19.7   Unless this information is regularly updated, the ability of CSOs and SSOs to communicate with PFSOs and national contact points is adversely affected particularly when updating SSAs or seeking advice on security issues.

2.19.8   To facilitate the exchange of the information specified in the Maritime Security Measures between Governments and the IMO, Governments have been asked to designate a single National Contact Point with responsibility for the exchange of the required information. The name and contact details must be kept updated.

Port facilities

2.19.9   Governments are also required to provide the IMO with up-to-date information on their designated port facilities. The template designed for this purpose is included as Appendix 2.13 – Details of Port Facilities and includes such details as:

- a   Location;
- b   Name of security point of contact (typically the PFSO);
- c   Date of the original approval of the port facility security plan;
- d   Date of most recent review of the port facility security plan;
- e   Date of most recently issued Statement of Compliance, if applicable; and
- f   Date of any PFSP withdrawal or amendment.

2.19.10   Any changes including newly-listed port facilities, location covered by an approved PFSP and withdrawal of an approved PFSPs should be provided at the earliest opportunity along with the date when the change took effect.

2.19.11   Governments are required to provide an updated list of their ISPS Code-compliant port facilities at five yearly intervals. The next updated list has to be submitted by 1 July 2014.

2.19.12   SOLAS chapter XI-2, regulation 13 requires that Contracting Government communicate to the Organization information on:

- a   The names and contact details of their national authority or authorities responsible for ship and port facility security;
- b   The locations within their territory covered by the approved port facility security plans;
- c   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;
- d   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; and
- e   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.

2.19.13   The information listed under paragraph 2.19.12 can be submitted to IMO by making appropriate entries into its GISIS database. GISIS comprises a number of modules and the relevant module for communicating information in accordance with SOLAS chapter XI-2, regulation 13 is the Maritime Security Module. The IMO Secretariat has recently amended the information to be provided for Contracting States' port facilities and is reflected in Appendix 2.13 – Details of Port Facilities.

National legislation

2.19.14   Under the SOLAS Convention, Governments are required to transmit to the IMO: "….the text of laws, decrees, orders and regulations which have been promulgated on the various matters within the scope of the present Convention."

2.19.15   Experience to date indicates that few Governments have provided copies of the required texts.

Additional information

2.19.16   Governments are required to provide the name and contact details of any RSO authorized to act on their behalf together with details of its delegated responsibilities and any conditions attached to the exercise of such authority.

2.19.17   As described in sub-section 2.13, Governments that have concluded an Alternative Security Agreement are required to provide the IMO with the information listed in paragraph 2.13.13.

2.19.18   As described in sub-section 2.14, Governments that have allowed any Equivalent Security Arrangements at port facilities or on ships are required to provide the IMO with the information listed in paragraph 2.14.6.

Appendix 2.1 – Implementation Questionnaire for Designated Authorities

Source: MSC.1/Circ.1192, May 2006

This questionnaire may be used by Designated Authorities to examine the status of implementation of the government's responsibilities for port facility security as specified in the Maritime Security Measures. When completing the questionnaire, the answers should be sufficiently detailed in order to gain a full understanding of the approach taken by the Contracting Government in implementing the Maritime Security Measures and prevent the drawing of erroneous conclusions.

Implementation Process

1   Who is the Designated Authority? (SOLAS regulation XI-2/1.11)

2.   What is the national legislative basis for the implementation of the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)

3.   What guidance to industry was released to implement the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)

4.   What are the means of communication with port facilities regarding ISPS Code implementation? (SOLAS regulations XI-2/3 and XI-2/10)

5.   What processes are in place to document initial and subsequent compliance with the ISPS Code? (SOLAS regulation XI-2/10.2)

6.   What is the Contracting Government's definition of a Port Facility? (SOLAS regulation XI- 2/1.1)

7.   What are the procedures used to determine the extent to which port facilities are required to comply with the ISPS Code, with particular reference to those port facilities that occasionally serve ships on international voyages? (SOLAS regulations XI-2/1, XI-2/2.2)

8.   Has the Contracting Government concluded in writing bi-lateral or multi-lateral agreements with other Contracting Governments on alternative security agreements? (SOLAS regulation XI-2/11.1)

9   Has the Contracting Government allowed a port facility or group of port facilities to implement equivalent security arrangements? (SOLAS regulation XI-2/12.1)

10.   Who has the responsibility for notifying and updating the IMO with information in accordance with SOLAS regulation XI-2/13? (SOLAS regulation XI-2/13)

Port Facility Security Assessment (PFSA)

11.   Who conducts PFSAs? (SOLAS regulation XI-2/10.2.1, ISPS Code sections A/15.2 and 15.2.1)

12.   How are PFSAs conducted and approved? (ISPS Code sections A/15.2 and 15.2.1)

13.   What minimum skills are required for persons conducting PSFAs? (ISPS Code section A/15.3)

14.   Are PFSAs used for each Port Facility Security Plan? (ISPS Code section A/15.1)

15.   Do single PFSAs cover more than one port facility? (ISPS Code section A/15.6)

16.   Who is responsible for informing the IMO if the single PFSA covers more than one port facility? (ISPS Code section A/15.6)

17.   What national guidance has been developed to assist with the completion of PFSAs? (SOLAS regulation XI-2/10.2.1)

18.   What procedures are in place for determining when re-assessment takes place? (ISPS Code section A/15.4)

19.   What procedures are in place for protecting the PFSAs from unauthorized access or disclosure? (ISPS Code section A/15.7)

Port Facility Security Plans (PFSPs)

20.   How are Port Facility Security Officers designated? (ISPS Code section A/17.1)

21.   What are the minimum training requirements that have been set by the Contracting Government for PFSOs? (ISPS Code section A/18.1)

22.   Are procedures used to determine the individuals/organizations responsible for the preparation of the PFSP? If yes, please describe.

23.   Are procedures in place to protect PFSPs from unauthorized access? (ISPS Code sections A/16.7 and A/16.8)

24.   What procedures are in place for approval and subsequent amendments of the PFSPs? (ISPS Code section A/16.6)

Security Levels

25.   Who is the authority responsible for setting the security level for port facilities? (SOLAS regulation XI-2/3.2)

26.   What are the procedures for communicating security levels to port facilities by the responsible authority? (SOLAS regulation XI-2/3.2)

27.   What are the procedures for communicating port facilities' security levels to ships? (SOLAS regulations XI-2/4.3 and XI-2/7.1)

28.   What are the contact points and procedures for receiving ships' security level information in the Contracting Government and for notifying ships of contact details? (SOLAS regulation XI-2/7.2)

Declaration of Security

29.   What procedures are used to determine when a Declaration of Security is required? (SOLAS regulation XI-2/10.3, ISPS Code section A/5.1)

30.   What is the minimum timeframe that a Declaration of Security is required to be retained? (ISPS Code section A/5.6)

Delegation of Tasks and Duties

31.   What tasks and duties have the contracting government delegated to Recognized Security Organizations (RSOs) or others? (ISPS Code section A/4.3)

32.   To whom have these tasks and duties been delegated? What oversight procedures are in place? (SOLAS regulation XI-2/13.2)

Appendix 2.2 – Implementation Questionnaire for Administrations

Source: MSC.1/Circ.1193, May 2006

This questionnaire may be used by Designated Authorities to examine the status of implementation of the government's responsibilities for ship security as specified in the Maritime Security Measures. When completing the questionnaire, the answers should be sufficiently detailed in order to gain a full understanding of the approach taken by the Contracting Government in implementing the Maritime Security Measures and prevent the drawing of erroneous conclusions.

Implementation Process

1.   What is the national legislative basis for the implementation of the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/4)

2.   What guidance to industry was released to implement the ISPS Code? (SOLAS regulations XI-2/2, XI-2/4, XI-2/5 and XI-2/6)

3.   What are the means of communication developed by the Administration with (a) ships, and (b) companies, regarding ISPS Code implementation? (SOLAS regulations XI-2/3 and XI-2/4)

4.   What processes are in place to document verification and certification of initial and subsequent compliance with the ISPS Code? (SOLAS regulation XI-2/4.2)

5.   Has the Contracting Government nominated a point of contact for ships to request assistance or report security concerns? If yes, provide the name and contact details. (SOLAS regulation XI-2/7.2)

6.   Have officers been duly authorized to exercise control and compliance measures on security grounds and has guidance been issued to them? (SOLAS regulation XI-2/9)

7.   Has guidance been issued to companies and ships on the provision of information to other Contracting Governments when applying control and compliance measures, including the records to be retained by the ship in respect of the last ten calls at port facilities? (SOLAS regulation XI-2/9)

8.   Has the Contracting Government concluded in writing bilateral or multilateral agreements with other Contracting Governments on alternative security agreements? (SOLAS regulation XI-2/11.1)

9.   Has the Administration allowed a ship or group of ships to implement equivalent security arrangements? (SOLAS regulation XI-2/12.1)

10.   Who has the responsibility for notifying and updating the IMO with information in accordance with SOLAS regulation XI-2/13? (SOLAS regulation XI-2/13)

Ship Security Assessment (SSA)

11.   Who conducts SSAs? (ISPS Code sections A/8.2 and 8.3)

12.   Has national guidance been developed to assist with the completion of the on-scene security survey? (ISPS Code section A/8.4)

Ship Security Plans (SSPs)

13.   Who approves SSPs? (ISPS Code sections A/9.1 and 9.2)

14.   How are Company and Ship Security Officers designated? (ISPS Code sections A/11.1 and A/12.1)

15.   What are the minimum training requirements that have been set by the Administration for CSOs and SSOs? (ISPS Code sections A/13.1 and A/13.2)

16.   Has guidance been issued on the development and approval of SSPs (ISPS Code sections A/9.2 and 9.4)

17.   Are procedures in place to protect SSPs from unauthorized access? (ISPS Code section A/9.7)

18.   What procedures are in place for approval and subsequent amendments of the SSPs? (ISPS Code sections A/9.5 and 9.5.1)

19.   Do SSPs contain a clear statement emphasizing the master's authority? (ISPS Code section A/6.1)

20.   Is the original or a translation of the SSP available in English, French or Spanish? (ISPS Code section A/9.4

21.   Who verifies SSPs? (ISPS Code section A/19.1.2)

22.   Has the Administration specified the periods when renewal, intermediate and additional verifications shall be carried out? (ISPS Code section A/19.1.1)

23.   Who issues the International Ship Security Certificate (ISSC)? (ISPS Code section A/19.2.2)

24.   Has the Administration specified the period of validity of ISSCs? (ISPS Code section A/19.3.1)

25.   Does the Administration have procedures in place for the issue of Interim ISSCs? (ISPS Code section A/19.4)

26.   Has the Administration specified the minimum period for which records of activities addressed in the SSP shall be kept on board? (ISPS Code section A/10.1)

Security Levels

27.   Who is the authority responsible for setting the security level for ships? (SOLAS regulationXI-2/3.1)

28.   What are the procedures for communicating security levels to ships by the responsible authority? (SOLAS regulation XI-2/3.1)

29.   Have procedures been notified for a ship to comply with the security level set by the Contracting Government for a port facility whose security level is higher than set for the ship by the Administration? (SOLAS regulations XI-2/4.3 and XI-2/4.4)

30.   Are procedures in place to provide advice to ships in cases where a risk of attack has been identified? (SOLAS regulation XI-2/7.3)

Declaration of Security

31.   What procedures are used to determine when a Declaration of Security is required? (ISPS Code section A/5.1)

32.   What is the minimum time frame that a Declaration of Security is required to be retained? (ISPS Code section A/5.7)

Delegation of Tasks and Duties

33.   What tasks and duties, if any, have the Administration delegated to Recognized Security Organizations (RSOs)? (ISPS Code section A/4.3)

34.   To whom have these tasks and duties been delegated? Based on what criteria and under what conditions has the status of RSO been granted by the Administration to those organizations? What oversight procedures are in place? (SOLAS regulation XI-2/13.2)

35.   What procedures are in place to ensure that the RSO undertaking the review and approval process for an SSP was not involved in the preparation of the SSA or SSP? (ISPS Code section A/9.2.1)

Source: MSC /Circ.1074, June 2003

Demonstrating Organizational Effectiveness

- Clear lines of managerial oversight for the proposed delegation of authority;

- Relevant qualifications and experience of key personnel proposed for the delegation of authority including security clearances – these should be matched with their proposed work assignments;

- Planned training of key personnel during the duration of the delegation to ensure that qualifications are maintained and upgraded as necessary;

- Replacement strategy for key personnel;

- Company code of ethics or code of conduct;

- Successful testing of procedures established to avoid unauthorized disclosure of, or access to, security-sensitive material;

- Successful completion of similar activities to those identified in the proposed delegation of authority – this may require the RSO to identify recent examples of other national authorities which awarded similar delegations of authority;

- Adequate records management and internal quality control systems.

Demonstrating Technical Capabilities for Ship-related Delegations

- Appropriate knowledge of ship operations including design and construction considerations;

- Appropriate knowledge of the requirements and guidance specified in the Special Measures and relevant national legislation, regulations, policies and operating procedures;

- Appropriate knowledge of current security threats and patterns and their relevance to ship operations;

- Experience in the application and maintenance of security and surveillance equipment and systems installed on board ships

- Appropriate knowledge of their operational limitations including techniques used to circumvent them;

- Experience in assessing the likely security risks that could occur during ship operations including the ship/port interface and identifying options to minimize such risks.

Demonstrating Technical Capabilities for Port-related Delegations

- Appropriate knowledge of port operations including design and construction considerations;

- Appropriate knowledge of the requirements and guidance specified in the Special Measures and relevant national legislation, regulations, policies and operating procedures;

- Experience in assessing the likely security risks that could occur during port facility operations including the ship/port and identifying options to minimize such risks;

- Appropriate knowledge of current security threats and patterns and their relevance to port operations;

- Experience in the application and maintenance of security and surveillance equipment and systems installed in port areas;

- Appropriate knowledge of their operational limitations including techniques used to circumvent them.

Appendix 2.4 – Sample of a Port Facility Security Plan Approval Form

PORT FACILITY SECURITY PLAN APPROVAL FORM		File Number:	
Type of Port Facility:			
Name of Port Facility:			
Location			
Port ID Number:			
UN locator			
Statement of Compliance date of issue (yyyy-mm-dd):		Date of expiry (yyyy-mm-dd):	
Name of Operator:		Address of Operator:	
Telephone:	Fax:	E-mail:	
Name of PFSO:		24 hrs Contact Number:	
Telephone:	Fax:	E-mail:	
Designated Authority Security Office:	Address:		
Telephone:	Fax:	E-Mail:	
Approved Date:	Follow-up action required		Date reviewed:

_____   _____

Reviewed by: Print name   **Signature**

APPROVAL DOCUMENT SECTIONS

(Check the box when section completed)
Section 1 – Organizational Structure of the Port Facility
Section 2 – Security and Communication Equipment
Section 3 – Drills and Exercises
Section 4 – Records and Documentation
Section 6 – Security Procedures during Interfacing
Section 7 – Declarations of Security
Section 8 – Response to a Change in the Security level
Section 9 – Security Procedures for Access Control
Section 10 – Security Procedures for Restricted Areas
Section 11 – Security Procedures for Handling Cargo
Section 12 – Security Procedures for Delivery of Ships' Stores and Bunkers
Section 13 – Security Procedures for Monitoring
Section 14 – Response to Security Threats, Breaches of Security and Security Incidents
Section 15 – Audits and Amendments

Section 1 - Organizational Structure of the Port Facility		
The Plan identifies the:		
Requirement	**Plan Ref.**	**Yes/No**
Name of Security Organization		
Name of Operator		
Name and Position of PFSO & 24 hour contact information		
Duties and Responsibilities of the PFSO		
Duties and Responsibilities of Personnel with Security Responsibilities		
Training Requirements of the PFSO and port facility personnel with designated security responsibilities		
The security organization's links with other national or local authorities with security responsibilities		
Comments:		

Section 2 – Security and Communication Equipment		
The Plan includes:		
Requirement	**Plan Ref.**	**Yes/No**
Procedures for maintaining security and communication systems and equipment		
Procedures for identifying and correcting security equipment or systems failures or malfunctions		
A description of security equipment for access control		
A description of security equipment for monitoring the port facility and surrounding area		
A description of how monitoring is achieved by any combination of lighting, security guards on foot or in vehicles, waterborne patrols, automatic intrusion-detection devices and surveillance equipment		
If an automatic intrusion-detection device is used, it activates an audible or visual alarm, or both, at a location that is continuously attended or monitored		
Monitoring is able to function continuously, including during periods of adverse weather or power disruption		
Monitoring equipment covers access and movements adjacent to ships interfacing with the port facility		
Comments:		

Section 3 - Drills and Exercises		
The Plan includes provision for:		
Requirement	**Plan Ref.**	**Yes/No**
Security drills to be conducted every three months		
Security drills to test individual elements of the PFSP, including the response to security threats, breaches of security and security incidents, taking into account the types of operations, personnel changes, the types of ships interfacing with the facility and other relevant circumstances		
Security exercises to fully test the PFSP, including the active participation of facility personnel who have security responsibilities, relevant government officials, the CSO and any available ship security officers		
Security exercises to check communication and notification procedures, elements of		

coordination, resource availability and response		
Security exercises to be conducted at least once every calendar year with no more than 18 months between them.		
Comments:		

Section 4 - Records and Documentation		
The Plan includes provision for the PFSO to keep the following records:		
Requirement	**Plan Ref.**	**Yes/No**
Rate of inspections specified in the Plan		
Security training, including dates, duration, description and names of participants		
Security drills & exercises, including dates, description, names of participants and any best practices or lessons learned		
Security threats, breaches of security and security incidents, including date, time, location, the response to them and the person to whom they were reported		
Changes in the security level, including the date, time that notification was received and the time of compliance with the requirement of the new level		
Maintenance, calibration and testing of equipment used for security including the date and time of the activity and the equipment involved		
Declarations of security in respect of the port facility		
Internal audits and reviews of security activities		
Security assessment information, including the PFSA, each periodic review, the dates conducted and their findings		
The Plan, including each periodic review date conducted, their findings and any recommended amendments		
Amendments to the Plan, including the date of its approval and implementation		
Records of inspections and patrols		
A list, by name or position, of the persons who have security responsibilities		
An up-to-date list containing the names of screening officers (if applicable)		
For at least two years and to be available to government officials on request. In the case of the Plan and its related PFSA, the retention time is for at least two years after the Plan's expiry date		
Protected from unauthorized access or disclosure, including the Plan		
If in electronic format, protected from deletion, destruction and revision		
Comments:		

Section 5 - Communications		
The Plan addresses (as per Section 323):		
Requirement	**Plan Ref.**	**Yes/No**
Procedures that allow for effective communications between personnel with security responsibilities with respect to the ships interfacing with the facility and with port operators, if applicable, the Designated Authority and local law enforcement agencies		
The means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches		
Back-up communications to ensure internal and external communications		
Comments:		

Section 6 - Security Procedures during Interfacing		
The Plan includes procedures for		
Requirement	**Plan Ref.**	**Yes/No**
Coordinating with ships interfacing with the port facility and the port operator, if applicable.		
Assisting SSOs in confirming the identity of those seeking to board the ship when requested		
Facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organizations.		
Comments:		

Section 7 - Declarations of Security		
The Plan makes provision for		
Requirement	**Plan Ref.**	**Yes/No**
The requirements and procedures for completing Declarations of Security		
A DOS to be completed before an interface starts between a port facility and a ship if they are operating at different Security levels		
A DOS to be completed before an interface starts between a port facility and a ship if one of them does not have an approved security plan		
A DOS to be completed before an interface starts between a port facility and a ship if the interface involves a cruise ship, a ship carrying dangerous goods or the loading or transfer of dangerous goods		
A DOS to be completed before an interface starts between a port facility and a ship if the security officer of either of them identifies security concerns about the interface		
Comments:		

Section 8 - Response to a Change in the Security level		
The Plan contains procedures for ensuring that, when the operator of the port facility is notified of an increase in the Security level:		
Requirement	**Plan Ref.**	**Yes/No**
The port facility complies with the required additional security procedures within the specified time period after the notification		
The Designated Authority receives a report indicating compliance or noncompliance with the Security level		
If the increase is to Security level 3, the port facility evaluates the need for additional security procedures		
Comments:		

Section 9 - Security Procedures for Access Control		
The Plan includes procedures for:		
Requirement	**Plan Ref.**	**Yes/No**
At all Security levels: • preventing unauthorized access to the port facility by persons, weapons, incendiaries, explosives, dangerous substances and devices		

Requirement	Plan Ref.	Yes/No
At Security Level 1:		
• Establishing control points for restricted access that should be bounded by fencing or other barriers	•	•
• Verifying the identity of every person seeking to enter a controlled access area and the reasons for which they seek entry	•	•
• Screening of persons, goods and vehicles for weapons, explosives or incendiaries at the rate specified in the Plan	•	•
• Checking vehicles used by those seeking entry to the port facility	•	•
• Verifying the identity of port facility personnel and those employed within the port facility, and their vehicles	•	•
• Restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity	•	•
• Searches of persons, personal effects, vehicles and their contents at the rate specified in the Plan	•	•
• Denying or revoking of a person's authorization to enter or remain on a port facility if they are not authorized or fail to identify themselves.	•	•
• Determining the appropriate access controls for deterring unauthorized access to the port facility including its restricted areas	•	•
• Identifying access points that must be secured or attended to deter unauthorized access	•	•
• Screening or searching unaccompanied baggage at the rate(s) specified in the Plan	•	•
Requirement	**Plan Ref.**	**Yes/No**
At Security Level 2:		
• Increasing the frequency of screening persons and goods	•	•
• Authorized screening of all unaccompanied baggage by means of x-ray equipment	•	•
• Additional personnel to guard access points and for perimeter patrols	•	•
• Limiting the number of access points to the port facility	•	•
• Impeding movement through the remaining access points, e.g. security barriers	•	•
• Increasing the frequency of searches of persons, personal effects and vehicles	•	•
• Denying or revoking access to persons who are unable to provide a verifiable justification for seeking access	•	•
• Coordinating with the Designated Authority, appropriate law enforcement agencies, port operator, if applicable, to deter waterside access to the facility	•	•
Requirement	**Plan Ref.**	**Yes/No**
At Security Level 3:		
• Additional screening of unaccompanied baggage	•	•
• Coordinating with emergency response personnel and other port facilities	•	•
• Granting access to those responding to the security incident or security threat	•	•
• Suspending all other access to the port facility	•	•
• Suspending cargo operations within all, or part, of the port facility	•	•
• Evacuating the port facility or part thereof	•	•
• Restricting pedestrian and vehicular movements	•	•
• Increasing monitoring of the security patrols within the port facility, if appropriate	•	•
• Directing all movements relating to all, or part, of the port facility	•	•
Comments:		

Section 10 - Security Procedures for Restricted Areas		
The Plan makes provision for designating restricted areas, including those listed below, and specifying measures and procedures, as appropriate to the facility's operations at each Security level		
Requirement	**Plan Ref.**	**Yes/No**
Land areas adjacent to ships interfacing with the port facility		
Embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas, including search points		
Areas designated for loading, unloading or storage of cargo and ships' stores		
Areas in which security-sensitive information is kept, including cargo documentation		
Areas where dangerous goods and hazardous substances are held		
Vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms		
Areas where security and surveillance equipment is stored or located		
Essential electrical, radio and telecommunication, water and other utility installations		
Locations in the port facility where it is reasonable to restrict access by vehicles and persons		
At Security Level 1:		
• Providing permanent or temporary barriers to surround the restricted area.		
• Procedures for securing all access points not actively used and providing physical barriers or security guards to impede movement through the remaining access points		
• Procedures for controlling access to restricted areas, such as a pass system that identifies an individual's entitlement to be within the restricted area.		
• Procedures for examining the identification and authorization of persons and vehicles seeking entry, and clearly marking vehicles allowed access to restricted areas		
• Procedures for patrolling or monitor the perimeter of restricted areas		
• Procedures for using security personnel, automatic intrusion detection devices or surveillance equipment/systems to detect unauthorized entry or movement in the restricted areas		
• Procedures for controlling the movement of vessels in the vicinity of ships using the port facility		
• Procedures for designating temporary restricted areas, if applicable, to accommodate port facility operations, including restricted areas for segregating unaccompanied baggage that has undergone authorized screening by a ship operator		
• Procedures for conducting a security sweep (both before and after) if a temporary restricted area is designated		
At Security level 2:		
• Procedures for enhancing physical barriers, use of patrols or intrusion detection devices		
• Procedures for reducing the number of access points and enhancing controls applied at the remaining access points		
• Procedures for restricting parking of vehicles adjacent to ships		
• Procedures for reducing access to restricted areas and movements and storage in them		
• Procedures for using surveillance equipment that records and monitors continuously		
• Procedures for increasing the number and frequency of patrols, including the use of waterside patrols		
• Procedures for establishing and restricting access to areas adjacent to restricted areas		
• Enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility		
At Security Level 3:		
• Procedures for designating additional restricted areas adjacent to the security incident or threat to which access is denied		
• Procedures for searching restricted areas as part of a security sweep of all or part of the port facility		

Comments

Section 11 - Security Procedures for Handling Cargo

The Plan includes procedures for:

Requirement	Plan Ref.	Yes/No
Identifying cargo that is accepted for loading onto ships interfacing with the port facility		
Identifying cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up		
At Security Level 1:		
• Verifying that cargo, containers and cargo transport units entering the port facility match the invoice or other cargo documentation		
• Routine inspection of cargo, containers, transport units and cargo storage areas before and during handling operations to detect evidence of tampering, unless unsafe to do so		
• Verifying that the cargo entering the facility matches the delivery documentation		
• Searching vehicles entering the port facility		
• Examining seals and other methods used to detect evidence of tampering when cargo, containers or cargo transport units enter the port facility or are stored there		
At Security Level 2:		
• Detailed checking of cargo, containers, and cargo transport units in or about to enter the port facility or cargo storage areas, for weapons, explosives and incendiaries		
• Intensified inspections to ensure that only documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship		
• Detailed search of vehicles for weapons, explosives and incendiaries		
• Increasing the frequency and detail of examinations of seals and other methods used to prevent tampering		
• Increasing the frequency and intensity of visual and physical inspections		
• Increasing the frequency of the use of scanning/detection equipment, mechanical devises or dogs.		
• Coordinating enhanced security measures with shippers or those acting on their behalf in accordance with an established agreement and procedures		
At Security Level 3:		
• Restricting or suspending cargo movements or operations in all or part of the port facility		
• Confirming the inventory and location of certain dangerous cargoes in the port facility		

Comments

Section 12 - Security Procedures for Delivery of Ships' Stores and Bunkers

The Plan include procedures for:

Requirement	Plan Ref.	Yes/No
At Security Level 1:		
• Checking ship stores		
• Requiring advanced notification of the delivery of ships' stores or bunkers, including a list of stores, and driver and vehicle registration information in respect of delivery vehicles		
• Inspecting delivery vehicles at the rate specified in the Plan		
At Security Level 2:		
• Detailed checking of ship's stores		
• Detailed searches of delivery vehicles		

Requirement	Plan Ref.	Yes/No
• Coordinating with ship personnel to check the order against the delivery note prior to entry to the port facility		
• Escorting delivery vehicles in the port facility		
At Security Level 3:		
• Restricting or suspending the delivery of ships' stores and bunkers		
• Refusing to accept ships' stores in the port facility		
Comments		

Section 13 - Security Procedures for Monitoring

The Plan establishes the procedures and equipment needed at each Security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or of power disruptions, including:

Requirement	Plan Ref.	Yes/No
At Security Level 1:		
• the security measures to be applied, which may be a combination of lighting, security guards or use of security and surveillance equipment to allow port facility security personnel to:		
- Observe the general port facility area, including shore- and water-side accesses to it;		
- Observe access points, barriers and restricted areas; and		
- Allow port facility security personnel to monitor areas and movements adjacent to ships, including augmentation of lighting provided by the ship itself.		
At Security Level 2:		
• Additional procedures to increase the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance		
• Procedures for increasing the frequency of foot, vehicle or waterborne patrols		
• Procedures for assigning additional security personnel to monitor and patrol		
At Security Level 3:		
• Procedures for switching on all lighting in, or illuminating the vicinity of, the port facility		
• Procedures for switching on all surveillance equipment capable of recording activities in or adjacent to the port facility		
• Procedures to maximize the length of time that surveillance equipment can continue to record		
Comments		

Section 14 - Response to Security Threats, Breaches of Security and Security Incidents

The Plan addresses procedures for:

Requirement	Plan Ref.	Yes/No
At all Security levels,		
• Responding to security threats, breaches of security and security incidents, including provisions to maintain critical port facility and interface operations		
• Evacuating the port facility in case of security threats and security incidents		
• Reporting security threats, breaches of security, and security incidents to the Designated Authority		
• Briefing port facility personnel on potential threats to security and the need for vigilance		
• Securing non-critical operations in order to focus response on critical operations		
• Reporting security threats, breaches of security and security incidents to the appropriate law enforcement agencies, the Designated Authority and, if applicable, the port operator		

Comments

Section 15 - Audits and Amendments

The Plan addresses when an audit is required and the timing for submitting audit-based amendments, as follows:

Requirement	Plan Ref.	Yes/No
The PFSA relating to the facility is altered		
An independent audit or the Designated Authority's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant elements of the approved Plan		
Security incidents or threats involving the port facility have occurred		
There is a new operator of the port facility, a change in operations or location, or modifications to the port facility that could affect its security		
If the audit results require an amendment to be made to the PFSA or Plan, the PFSO submits an amendment to the Designated Authority for approval within 30 days after completion of the audit		
If the operator of a port facility submits other amendments to the approved Plan, they are to be submitted at least 30 days before they take effect		
Comments		

PFSP REVIEW

APPROVED …………………………………………………….

DISAPPROVED……………………………………………….

COMMENTS_____
_____
_____
_____
_____

Appendix 2.5 – Statement of Compliance of a Port Facility

Source: Part B of the ISPS Code

Statement Number……………………………………..

Issued under the provisions of Part B of the International Ship and Port Facility Security (ISPS) Code by the Government of [*insert name and official seal, if appropriate*]

Name of the port facility…………………………………………………………………….

Address of the port facility…………………………………………………………………..

THIS IS TO CERTIFY that:

- the compliance of this port facility with the provisions of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code has been verified; and

- this port facility operates in accordance with its approved Port Facility Security Plan (PFSP). This plan has been approved for the types of operations, types of ship or activities or other relevant information listed below (delete non-applicable categories):
    - Passenger ship
    - Passenger high-speed craft
    - Cargo high-speed craft
    - Bulk carrier
    - Oil tanker
    - Chemical tanker
    - Gas carrier
    - Mobile offshore drilling units
    - Cargo ships other than those referred to above

This Statement of Compliance is valid until ……………………………., subject to verifications (as indicated overleaf)

Issued at …………………………………………………….
(place of issue)

Date of issue……………………………………………………

………………………………………………………………..

(Signature of the duly authorized official issuing the document)

(Seal or stamp of the issuing authority, as appropriate)

Endorsement for verifications

The Government of *[insert name]* has established that the validity of this Statement of Compliance is subject to [*insert relevant details of the verifications e.g. mandatory annual or unscheduled*].

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph 16.62.4 of Part B of the ISPS Code, the port facility was found to comply with the relevant provisions of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

1st VERIFICATION

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

Place: …………………………………………………

Date: ………………………………………………….

2nd VERIFICATION

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

Place: …………………………………………

Date: …………………………………………..

3rd VERIFICATION

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

Place: …………………………………………..

Date: …………………………………………..

4th VERIFICATION

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

Place: …………………………………………..

Date: …………………………………………..

Source: Part A of the ISPS Code

INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal)   *(State)*

Certificate Number:

Issued under the provisions of the

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

Under the authority of the Government of _____

(name of State)

by _____

(persons or organization authorized)

Name of ship: ……………………………………………............
Distinctive number or letters: ……………………………………………….................
Port of registry: ………………………………………………….............
Type of ship: ………………………………………………….............
Gross tonnage: ………………………………………………………….
IMO Number: ……………………………………………….………………..
Name and address of the Company: ..………………………………………………………

THIS IS TO CERTIFY:

1.   that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2.   that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3.   that the ship is provided with an approved Ship Security Plan.

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

This Certificate is valid until ………………………………………………………………………, subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at ……………………………………….....................................

(place of issue of the Certificate)

Date of issue ………………………............

……………………………………………………....................................

(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevantprovisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate verification   Signed …………………………….............................

                                                    (Signature of authorized official)

                                   Place …………………………..

                                   Date ……………………………

                                   (Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS*

Additional verification   Signed ………………………….............................

                                                    (Signature of authorized official)

                                   Place …………………………..

                                   Date ……………………………

                                   (Seal or stamp of the authority, as appropriate)

Additional verification   Signed ………………………….............................

                                                    (Signature of authorized official)

                                   Place …………………………..

                                   Date ……………………………

                                   (Seal or stamp of the authority, as appropriate)

Additional verification   Signed ………………………….............................

                                                    (Signature of authorized official)

                                   Place …………………………..

                                   Date ……………………………

                                   (Seal or stamp of the authority, as appropriate)

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

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

Signed …………………………………......................

(Signature of authorized official)

Place …………………………………............

Date …………………………………............

(Seal or stamp of the authority, as appropriate)

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

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

Signed …………………………………..

(Signature of authorized official)

Place …………………………………......................

Date …………………………………......................

(Seal or stamp of the authority, as appropriate)

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

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

Signed …………………………………............................

(Signature of authorized official)

Place …………………………………............................

91

Date …………………………….....................................

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE

UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE

SECTION A/19.3.6 OF THE ISPS CODE APPLIES

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

Signed ……………………………….....................................

(Signature of authorized official)

Place ………………………………….....................................

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE

WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

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

Signed ……………………………….....................................

(Signature of authorized official)

Place ………………………………….....................................

Date …………………………….....................................

(Seal or stamp of the authority, as appropriate

---

*   *Delete as appropriate.*

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

Source: Part A of the ISPS Code

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal)   *(State)*

Certificate No.

Issued under the provisions of the

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

Under the authority of the Government of _____

(name of State)

by _____

(persons or organization authorized)

Name of ship	: …....................……...
Distinctive number or letters	: …...
Port of registry	: …...…
Type of ship	: …………….…...
Gross tonnage	: …..
IMO Number	: …..…
Name and address of company	: …...…

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

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

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

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

This Certificate is valid until …...

Issued at …...

(place of issue of the certificate)

Date of issue ….................................   ….............................…...

(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

* Delete as appropriate

Administrations may wish to include any specific requirements (e.g. security records have to be maintained for 12 months) they have regarding ship security into the check list's generic questions. Administrations may also wish to provide guidance on which questions are applicable to initial, intermediate, renewal and additional inspections.

As an alternative to the format provided Administrations may wish amend the inspection details, change the order of questions to suit their inspection process, or add separate comments sheets and use the question number as the cross reference as opposed to having space for comments against each question.

SHIP SECURITY INSPECTION DETAILS	
Ship name	
IMO number	
Type of vessel	
Date of inspection	
Place of inspection	
Type of inspection	Initial / Intermediate / Renewal / Additional
Company name	
Company ID number	
Company Security Officer name	
Master name	
Ship Security Officer name	

Questions	Yes/No	Comments
APPROACHING THE SHIP		
1) Is **Ship Identification Number** marked as defined in SOLAS XI-1/3		
Access Control (preventing unauthorised access and articles)		
2) Are procedures implemented for identification for ship's personnel, passengers and visitors, as specified in SSP?		
3) If a pass system is defined in the SSP is it implemented?		
4) If a pass system is defined in the SSP, are crew passes withdrawn when that person leaves ship permanently?		
5) If a pass system is defined in the SSP, are visitor or contractor passes withdrawn on exiting the ship?		
6) Are the Ship's deck and access points illuminated?		
7) Is there controlled access to the ship?		
8) Is there effective control of the embarkation of persons and their effects?		
9) Is checking of identification of all persons seeking to board the ship carried out?		
10) Are Inspections and searching of persons carried out in designated areas (as applicable)?		
11) Are access points that should be secured or attended secured or attended?		
12) Is 'search' signage as defined in SSP in place?		

13) **For Ro-Ro ships**, is the frequency for searching vehicles for the designated ship as described in the SSP maintained (as applicable)?		
14) **For passenger ships,** are checked and unchecked persons segregated as well as embarking and disembarking passengers?		
15) **For passenger ships,** are the unattended spaces adjoining areas, to which passengers and visitors have access secured or locked?		
16) **For passenger ships,** is there at least one male and one female searcher at each access point?		
17) **For passenger ships,** do passengers have passes and return them when leaving the ship at the end of the voyage?		
18) **If the ship has operated at SL2,** have the addition protective access control measures defined in SSP been implemented?		
19) **If the ship has operated at SL3,** have the further specific protective access control measures defined in SSP been implemented?		
20) At SL3, are the provisions in the SSP for limited access by officers authorised understood?		
IN MASTER'S CABIN / SHIP'S OFFICE		
Certification and Ship Security Plan		
21) Is the **ISSC** an original version?		
22) Do the entries on ISSC agree with those on CSR, SMC and DOC?		
23) Is there an up to date **Continuous Synopsis Record** on board?		
24) Do the entries on the CSR agree with those on Certificate of Registry and Class Certificate?		
25) Is the version of SSP held on board the same as Administration's approved version?		
26) Is the SSP based on the current ship security assessment (SSA)?		
27) Are the SSP, SSA, and other associated material, protected from unauthorised access or disclosure?		
28) If the SSP is in electronic format, is it protected against unauthorised deletion, destruction or amendment?		
29) If the SSP is in electronic format, is the password changed regularly?		
30) Is the SSP is written in the working language of the ship (if not English, French or Spanish a translation has to be provided into one of these languages)?		
31) Is the organisational structure as described in SSP for security known, understood and implemented?		
32) Are the relationships with company, port facilities, other ships and relevant authorities known and understood by key personnel?		
33) Are the evacuation procedures in case of security threats or breaches of security known and implemented?		

34) Are SSP amendments or changes in the security equipment approved, if required, by the Administration?		
35) Are these changes are clearly identified in the SSP?		
36) Have any amendments to the SSP been implemented?		
37) Does the SSO understand the procedure to follow for changes?		
38) Are the company policy and objectives on security understood?		
39) Does the master understand the discretion available for safety and security?		
40) Has the company ensured that the necessary support is given to the CSO to enable the Master and SSO to fulfil their duties and responsibilities?		
41) Are contact points available for Flag State and other relevant contracting governments?		
Security Records		
42) Have Security records (training, drills and exercises; threats and incidents; breaches of security; change in SL; internal audits and reviews; implementation of SSP amendments, maintenance, calibration & testing of security equipment,) been kept up to date?		
43) Are security records kept for the length of time specified in the SSP?		
44) Are security records in ship's working language?		
45) Are records protected from unauthorised access or disclosure?		
46) When kept in electronic format, are records protected to prevent unauthorised deletion, destruction or amendment?		
Ship/Port and Ship/Ship Interface		
47) Has the ship has acted upon the security levels set by the Administration?		
48) Are procedures understood regarding instructions from Contracting Governments when at SL3?		
49) Is receipt of instructions by the Administration including change of the security levels acknowledged?		
50) Has the ship informed nearby Coastal States regarding operating at SL 2 or SL3, if applicable?		
51) Has the ship has acted upon the security levels set by the Contracting Government of ports?		
52) Is provision made to ensure that the ship does not have a lower SL than the Port Facility?		
53) Has Contracting Government and PFSO been informed if the ship is been at a higher security level than the port facility?		
54) Have the pre-arrival notifications been handled correctly?		
55) Have the procedures for interfacing with the port facility specified in the ship security plan been followed?		

56) Are Declarations of Security completed as defined in the SSP?		
57) Is the procedure understood regarding failure by the Port Facility or other ship to acknowledge a DOS?		
58) Are appropriate ship security procedures maintained during any ship-to-ship interface?		
Security Training, Drills and Exercises		
59) Does the Ship Security Officer have a certificate of proficiency as SSO?		
60) Until 31/12/11, do crew understand - their responsibilities as described in the SSP and have sufficient knowledge to perform them? - the meaning and the consequential requirements of the different security levels? - knowledge of the emergency procedures and contingency plans? - recognition and detection of weapons, dangerous substances and devices? - techniques used to circumvent security measures?		
61) After 1/1/12, has familiarisation training for all personnel been carried out?		
62) After 1/1/12, do all crew have certificates of proficiency in security awareness?		
63) After 1/1/12, do all crew with designated security duties have certificates of proficiency in security duties?		
64) Are security briefings for the crew carried out?		
65) Have security drills been carried out as detailed in SSP?		
66) Have security exercises been carried out at the frequency shown in SSP?		
Responding to security threats and breaches of security		
67) Has the CSO obtained information on the assessments of threat for the ports of call and their protective measures and is this available on board?		
68) Is information available with respect to security threats from Contracting Governments?		
69) Are procedures for raising alarm for security threats or security incidents known and implemented?		
70) Are Procedures known, and can be implemented, for responding to security threats or breaches of security, including maintenance of critical operations of the ship or ship/port interface?		
71) Have any breaches of security been reported to the Administration, port facility, coastal state or CSO?		
72) Have breaches of security been investigated and mitigation measures implemented?		
73) Have potential on-board weapons that could be used by those committing a breach of security been identified?		
74) Are such potential weapons controlled to prevent their unauthorised use?		
Audit and Review		

75) Have internal audits been undertaken as required by the SSP?		
76) Have reviews of security been undertaken as required by the SSP?		
77) Have personnel been conducting internal audits of the security activities independent of the activities being audited? (unless this is impracticable due to the size and the nature of the company or of the ship)		
78) Have the Non-conformities of previous **internal** audits and reviews been properly dealt with?		
79) Have the Non-conformities of previous **external** audits been properly dealt with?		
TOUR OF SHIP		
Restricted Areas		
80) Are the restricted areas identified and known?		
81) Are the procedures in the SSP implemented to prevent unauthorised access to restricted areas?		
82) If coded key pads are used, is the code changed as required by the SSP?		
83) Are there any other ship critical areas that should be restricted areas?		
84) Are there other areas that require extra vigilance at heightened security levels (e.g. galley or crew mess)?		
85) Is functionality of emergency escapes maintaining while preventing unauthorised access to restricted areas?		
86) **If the ship has operated at SL2,** has the addition monitoring as defined in SSP been implemented?		
87) **If the ship has operated at SL3,** have measures been taken in co-operation with those responding to the incident or threat?		
Monitoring security		
88) Is there an effective deck watch while ship is in port or anchored off?		
89) Are areas surrounding the ship, particularly to seaward, monitored?		
90) Is there lighting on all decks and access points whilst berthed?		
91) Is CCTV used when available?		
92) Have patrols as detailed in the SSP been implemented?		
93) **For Ro-Ro ships**, are car decks monitored when loading and unloading?		
92) **If the ship has operated at SL2,** have the addition measures defined in SSP been implemented?		
93) **If the ship has operated at SL3,** have measures been taken in co-operation with those responding to the incident or threat?		
Handling of cargo, stores and unaccompanied baggage		
94) Is handling of **cargo** supervised as defined in the SSP?		

95) **For Ro-Ro ships**, are vehicles searched prior to loading according to the frequency in the SSP?		
96) Is handling of deck, engine-room and catering **stores** supervised as defined in the SSP?		
97) Is handling of **unaccompanied baggage** supervised as defined in the SSP?		
98) **If the ship has operated at SL2,** have the addition measures defined in SSP been implemented?		
99) **If the ship has operated at SL3,** have measures been taken in co-operation with those responding to the incident or threat?		
Security Equipment		
100) Can the sending of a test **SSAS** be demonstrated?		
101) Are Procedures (testing, activation, de-activation and resetting, limiting false alarms) understood for the use of the SSAS including location of activation buttons?		
102) Are tests of the SSAS conducted at the frequency specified in the SSP?		
103) Is any other security equipment inspected, tested and calibrated as applicable?		
104) Is all security equipment in working order?		
Communication		
105) Are the crew able to communicate on security issues?		
106) Is the CSO 24-hour contact known to key personnel?		

Appendix 2.9 – Sample of a Notice of Non-Compliance

Name of Ship	IMO Number	Type of Ship	Flag State	Date of Inspection	Place of Inspection		
Item Number		Deficiency			Regulatory reference	Due date	Date rectified	Date checked
1.								
2.								
X								

The information on this form is collected under the authority of …………………………………..

……………………………………………………………   ……………………………………

Signature of inspector (for the national authority)   *Date*

………………………………………………………….   ……………………………………

Signature of authorized representative acknowledging receipt   *Date*

Appendix 2.10 – Sample of a Core Training Curriculum for Officials in National Authorities

Core Training Element	Main Topics
Overview of International Maritime Security Framework	• IMO's role & structure, decision making process, member States, Conventions, Codes of Practice including ILO/IMO Code of Practice on Port Security • Port State Control MOUs • History of SOLAS Amendments 2002 • Role of regional organizations
Overview of National Authority's Legislative, Policy & Organizational Framework	• Legislation, Regulations & other legal instruments (including planned amendments) • Approval process • National policy statements • Inter-departmental/agency roles & coordination mechanisms • Bilateral & multilateral agreements • Organizational structure of national authority and link to responsible Minister
Overview of Maritime Industry under National Authority's Jurisdiction	• Key statistics on maritime trade, port activity and ship movements • Current & planned industry initiatives • Industry associations • Major security incidents
National Authority Responsibilities under SOLAS Amendments 2002 & ISPS Code	• List of responsibilities, comparison with port & shipping industry responsibilities and link to legislative framework (which may prescribe a broader set of responsibilities)
Responsibilities delegated to officials	• Delegation of Authority or equivalent document empowering officials • Official Identification cards • Delegations to RSOs
Code of Conduct	• National Authority's code of conduct
National Authority's Regulatory Oversight Program	• Program structure & elements • Ships, port facilities & other entities under the program's jurisdiction • Operational policies
Verification Procedures	• Pre-approval verification process including techniques and checklists • Post-approval/monitoring process including techniques and checklists • Report writing
Procedures for Handling Non-compliance	• Enforcement principles and continuum of enforcement actions • Techniques for handling non-compliance and promoting voluntary compliance • Forms & reports
Procedures for Observing or Participating in Exercises	• Types of exercises • Planning considerations and evaluating exercise results • Role of inspectors
Procedures for Administering Authorizations	• Certificate issuance process • Certificate renewal process
Procedures for Conducting Awareness & Education Activities	• Identifying target audiences • Types of delivery mechanisms • Promotional items

Appendix 2.11 – Sample of a Port Facility Security Inspection Report Form

PORT FACILITY SECURITY INSPECTION REPORT FORM		File Number:	
Type of Port Facility:			
Name of Port Facility:			
Location:			
Port ID Number			
UN Locator			
Statement of Compliance Number:		Security Level:	
Statement of Compliance date of issue (yyyy-mm-dd):		Date of expiry (yyyy-mm-dd):	
Name of Operator:		Address of Operator:	
Telephone:	Fax:	E-mail:	
Name of PFSO:		24 hrs Contact Number:	
Telephone:	Fax:	E-mail:	

Type of Inspection: □ Initial   □ Intermediate   □ Renewal
                      □ Additional (includes monitoring and follow-up)

Areas of Inspection (tick the appropriate boxes below):

□ 1. Documents and Records
□ 2. Access Control
□ 3. Restricted Area Access Control
□ 4. Handling of Cargo
□ 5. Delivery of Ships Stores and Bunkers
□ 6. Security Procedures for Monitoring
□ 7. Procedures for Threats and Security Incidents
□ 8. Security Communications
□ 9. Audits and Amendments
□ 10. Procedures for Shore Leave and Visitors to the Ship
□ 11. Procedures for Interfacing with Ship Security Activities
□ 12. Evacuation Procedures
□ 13. Security Procedures to Protect the Security Plan

Deficiencies Found
  □ Yes   □ No
		Supporting Documentation
		  □ Yes □ No	

Date of last Inspection (yyyy-mm-dd)		Have there been any changes to the port facility since the plan was approved?	
Security Office:	Address:		
Telephone:	Fax:	E-Mail:	
Date of Inspection (yyyy-mm-dd)	Name and signature of Inspector Name: Signature:		

Note: This inspection report must be retained at the port facility's office for a period specified by the Designated Authority and be available for consultation by a government official at all times.

1. Documents and Records	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:

- Does the PFSO keep the records or are they kept elsewhere? If so, has the PFSO documented their existence, location and the name/position of the person responsible? Verify.
- Are they complete as required and kept for at least 1 year? Verify
- Are the PFSP and related PFSA kept for at least 1 year after the day on which the PFSP expires? Verify.
- How are records protected from unauthorized access or disclosure? Verify.
- Are records kept electronically? If so, how are they protected from deletion, destruction and revision? Verify
- Are computer passwords protected and how often are they password changed? Verify.
- Interview port facility personnel to verify information recorded.

Observations:

Action required by Operator (if necessary):

Action by Inspector (if necessary):

2. Access Control	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:

- Gates/Barriers
  - Are gates secured (manned/locked)? Verify.
  - Do gates have card accesses?   Test card access with a number of cards.
  - Do gates have keys? Test keys of those authorized.
  - Inspect gates/barriers to ensure they are in good condition.
- Fencing
  - Inspect fences to ensure they are in good condition.
  - Verify that fences are clear of equipment/vehicles and debris against them.
  - Who patrols/checks the fences? Verify this with the person(s) named.
  - Who do personnel report breaches or damage to fencing to?
  - Are logs maintained for patrols of fence line or maintenance? Verify.
- Rail Security
  - Are access controls established where rail lines enter the facility? Verify.
  - Who monitors the activity at rail access points? Verify that they are monitored.
- Identification
  - Observe what types of ID are valid to access the port facility. What types of ID are valid to access the port facility? Verify that these types of ID are detailed in the PFSP.

When would a person be denied access to the facility or a restricted area? Is a log kept? Verify.

Observations:

Action required by Operator (if necessary):

Action by Inspector (if necessary):

3. Restricted Area Access Control	□ **Compliant** □ **Action Required**

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:

- What ID is valid to access or remain in a restricted area? Verify.
- What procedures are in place to issue passes, record their issuance, and record their loss? Verify.
- What procedures are in place for verifying the identity of government officials? Verify by interviewing a government official at the facility/vessel or through observation.
- What procedures are in place for verifying the identity of emergency responders?
- What procedures are in place for verifying visitors? Truck drivers? Crew? Verify through interview or observation.
- How are keys and passes controlled for restricted areas? Verify records.
- What is the process for reporting lost keys, passes or access cards? Is a record kept of those that are lost? Inspect it.
- Are persons subject to additional security measures when working in restricted areas? Verify through observation.
- Are persons entering the facility or restricted area recorded in a log? If so, verify the log.
- What is the procedure for crew access? What procedures are in place to ensure that only authorized crew are allowed back on the vessel? Verify this information with the SSO.
- What procedures are in place for visitors to access restricted areas or the vessel? Verify through observation where possible.

Observations

Actions Required by Operator (if necessary):

Actions Taken by Inspector (if necessary):

4. Handling of Cargo	□ **Compliant** □ **Action Required**

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:

- What procedures are followed to deter cargo tampering? Verify by observation.
- How is cargo identified and accepted for loading onto vessels? Verify through observation.
- How long cargo is stored at the facility prior to loading? Are there temporary storage areas? How is this cargo inspected prior to loading?
- Is there an inventory of dangerous cargoes? Are these cargos segregated from the remainder of the cargo at the port facility? Are they subject to additional security procedures? If so, are they detailed in the PFSP? Verify
- Are vehicles carrying cargo inspected? If so, how? Are these procedures detailed in the PFSP? Observe.

Observations

Action required by Port (if necessary):

Action by Inspector (if necessary):

5. Delivery of Ships Stores	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:
- How are security guards advised of ships' stores deliveries? Verify
- Are all ships' stores deliveries scheduled in advance?

Observations:

Actions Required by Operator (if necessary):

Actions Taken by Inspector (if necessary):

6. Security Procedures for Monitoring	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:
- Alarms, Motion Detectors and Lights
  - Who responds to alarm activations? Is the alarm company local? Do the alarms call the police?
  - Are they silent or audible? Inspect alarms by testing.
  - Where are the motion detection devices located? Inspect them by testing.
  - Who is responsible to ensure that facility lighting is in good working order? Verify
  - What are the maintenance procedures for alarms, motion detectors and lights? Verify.
- Control/Surveillance Rooms
  - Is this area restricted?
  - Is it signed? Verify signage.
  - Who has access? How is access controlled/secured? Verify.
  - How many persons are on duty throughout the day? Do they have other security responsibilities that may take them away from monitoring camera activity? Is the control room ever unattended?
  - How is the surveillance equipment maintained? Are records of maintenance and occurrences kept in the control room? Inspect records if kept in the control room.
  - Are images recorded when cameras are motion-activated, continuously recorded or not capable of recording?
  - What is the length of recording time? How long are the recordings kept before re-recording?
- Security Rounds
  - Who conducts security rounds? What do the security rounds entail? As part of security rounds, are passes verified and unfamiliar persons questioned?
  - Are the times and results recorded? Verify these records.
  - Are security sweeps conducted before (and/or after) a vessel interfaces with the dock? What is the procedure for security sweeps? Verify with facility personnel.
  - Are all restricted areas patrolled? If so, what is the frequency?
- Waterside Security
  - Who patrols the waterside of the port facility?
  - How does the PFSO contact the police or service provider for assistance? Verify contact number with PFSP.
  - Do security rounds include a patrol of the waterside and lands adjacent to the water? Who conducts patrols of the lands adjacent to the waterside? What is their frequency?

Are there surveillance cameras directed at the waterside of the port facility? Do they record activity? If so, how?

Observations:

Actions Required by Operator (if necessary):
Actions Taken by Inspector (if necessary):

7. Procedures for Responding to Security Threats, Breaches of Security and Security Incidents	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions :

- Reporting Security Incident and Threats
  - What are the procedures for reporting suspicious activities?
  - Do facility personnel use Security Incident Reports at the facility? Are these logged? Inspect the records. Are they submitted to the Designated Authority?
  - What procedures do facility personnel follow if they receive a bomb threat on their phone? Or discover a suspicious package on the dock? Or discover a suspicious person or activity occurring in the facility? Verify by asking facility personnel.
- Response Procedures
  - What is the responsibility of the PFSO when notified of an increase in Security level?
  - How does the PFSO respond to a specific security threat or breach?. Verify with the PFSP's response procedures.
  - How do personnel with security responsibilities respond to a specific security threat or breach? Verify that their response coincides with the PFSP's response.

Observations:
Actions Required by Operator (if necessary):
Actions Taken by Inspector (if necessary):

8. Security Communications	□ Compliant □ Action Required

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:

- Are personnel equipped with radios for security communication purposes?
- What channel is used for security communications? Verify with other personnel.
- Test the communication system and backup system (radio, telephone, etc.) by requesting the PFSO to contact someone on the facility or onboard the vessel.
- Are additional communication procedures put into effect when security levels increase? Verify.
- Where signs are used to advise facility personnel of a change in Security level, verify by inspecting the signs and asking personnel if they are aware of their usage.
- Ask personnel to identify the PFSO.
- Ask the PFSO if the vessel (or ship's agent) advises the facility of its Security level prior to arrival? How is this information communicated? Verify.
- What are the maintenance procedures for communications equipment? Verify.
- Ask the PFSO under what circumstances a DoS should be completed?
- Who has the authority to complete a DoS at the facility? Verify that this coincides with the security plan and/or persons listed.
- How are communication procedures established when a vessel interfaces? Verify this information with the SSO.
- If a radio or cellular phone is used, test this by requesting the PFSO to contact the vessel.
- How is the delivery and inspection of ships' stores coordinated? Verify this information with the SSO.

- How is information concerning the contact of reciprocal security officers, SSAS activation, security threats, breaches and incidents conveyed? Verify with the SSO.
- How is crew access is controlled? Verify with the SSO.

Observations:

Actions Required by Operator (if necessary):

Actions Taken by Inspector (if necessary):

9. Audits and Amendments	□ **Compliant** □ **Action Required**

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:
- Are annual audits of the PFSP based on the date of the original plan's approval?
- Do audits take place whenever there is a new operator, a change in operations or location, or modification to the port facility that could affect its security?
- Is there evidence of audits being undertaken in the form of audit plans, audit reports, meeting minutes, records of follow-up or remedial actions?
- Does the person who conducted the audit have the relevant formal qualifications and work experience? Verify by requesting examples of previous audit reports.

Observations:

Actions Required by Operator (if necessary):

Actions Taken by Inspector (if necessary):

10. Procedures for Shore Leave and Visitors to the Ship	□ **Compliant** □ **Action Required**

Plan References:

Possible questions for PFSO/security personnel and follow-up actions:
- What are the procedures in place for facilitating shore leave? Verify these with the PFSP.
- Who is responsible for escorting or continuously monitoring seafarers transiting through restricted areas of the port? Verify with security personnel identified as being responsible.

Observations:

Actions Required by Operator (if necessary):

Actions Taken by Inspector (if necessary):

11. Procedures for Interfacing with Ship Security Activities	□ **Compliant** □ **Action Required**

Plan References:

Possible questions for the PFSO/security personnel and follow-up actions:

Actions Required by Operator (if necessary):
Actions Taken by Inspector (if necessary):

12. Evacuation Procedures	□ Compliant □ Action Required
Plan References: Possible questions for PFSO/security personnel and follow-up actions:	
Observations:	
Actions Required by Operator (if necessary):	
Actions Taken by Inspector (if necessary):	

13. Security Procedures to Protect the Security Plan	□ Compliant □ Action Required
Plan References: • Is the PFSP made available only to people who have a legitimate need to know how to fulfil their official duties or contractual obligations? • Is the PFSP handled with due care and only in accordance with authorized procedures? • Is the PFSP kept in a safe place and accessed only in accordance with authorized procedures?	
Observations:	
Actions Required by Operator (if necessary):	
Actions Taken by Inspector (if necessary):	

Additional questions on qualifications of port facility personnel

For Port Facility Security Officer:

Q: What training have you received to become a PFSO?

For personnel with security responsibilities:

Q: What are your role and duties concerning security?

Q: What training have you received to perform these duties?

Q: How do your security duties change at Security levels 2 & 3?

For personnel without security responsibilities:

Q: What security orientation or training have you received?

Q: Do you have a facility identification card?

Q: What is a security level and what is the meaning of each level?

Q: What procedures are required of you at each Security level?

Additional Comments

Date	Comments

Appendix 2.12 – Details of National Authority Contact Points

Source: IMO Circular Letter No.2514, December 2003

1	Contact type*	
2	Organization/Authority/ Department	
3	First Name	
4	Surname	
5	Title	
6	Post	
7	Specific responsibilities	
8	Condition of Authority**	
9	Address	
10	Phone	
11	Fax	
12	Mobile	
13	E-mail	
14	Telex	

* One copy of Form is to be used for each organization according to its contact type:

1 National authorities responsible for ship security

2 National authorities responsible for port facility security

3 Proper recipients of SSAS alerts

4 Proper recipients of maritime security related communications from other Contracting Governments

5 Proper recipients of requests for assistance with security incidents

6 Names of Recognized Security Organizations (RSOs) approved by the State

** Condition of Authority is only applicable in the case of Recognized Security Organizations

Appendix 2.13 – Details of Port Facilities

1	Detail of the port	Name of port	
		Status*	
		Port ID number	
		UN Locator	
2	Port facility name		
3	Assigned port facility number**		
4	Alternative names for port (if applicable)		
5	Port facility description		
6	Location	Longitude	
		Latitude	
7	Port facility security point of contact		
8	Port facility taken part in alternative arrangement		
9	Port facility has approved port facility security plan		
10	Date of the original approval of the port facility security plan		
11	Date of most recent review of the port facility security plan		
12	Date of most recently issued Statement of Compliance, if applicable		
13	Has this port facility security plan been withdrawn?		
14	Port facility security plan withdrawn date		

*   Whether the port is open or closed

**   Port facility number should not be duplicated

Appendix 2.14 – Report of the Imposition of a Control and Compliance Measure

Source: MSC/Circ.1111, June 2004

(Reporting authority)

(Address)

(Telephone & Fax)

Copy to: Master

Duly Authorized Officer administrative office

If control measures, other than lesser administrative measures are taken, additional copies of this report shall be provided to:

Administration	☐
Recognized security organization	☐
IMO	☐
Port State of ship next port call (if denied entry or expelled)	☐

1. Name of reporting authority: _____
2. Date of inspection: _____
3. Place of inspection: _____
4. Name of ship: _____
5. Flag of ship: _____
6. Type of ship: _____
7. Call sign: _____
8. IMO Number: _____
9. Gross tonnage: _____
10. Year build: _____
11. Recognized security organization: _____
12. Registered owner (from Continuous Synopsis Record (CSR)): _____
13. Registered bareboat charterer, if applicable (from CSR): _____
14. Company (from CSR): _____
15. ISSC issuing Authority: _____
16. Dates of issue/expiry: _____
17. Ship security level: _____
18. Reason(s) for non-compliance: _____
_____
_____
_____
_____

19. Action taken by Duly Authorized Officer:
_____
_____

20. Specific control measures taken (marks as follow: "x" actions taken, "-" no actions taken)

None	☐
Lesser administrative measures	☐
More detailed inspection	☐
Ship departure delayed	☐
Restricted Ship Operation	
Cargo operation modified or stopped	☐
Ship directed to other location in port	☐
Ship detained	☐
Ship denied entry into port	☐
Ship expelled from port	☐

21. Corrective action taken by ship or Company:_____
_____
_____

Issuing office: _____

Name: _____

Telephone/Fax: _____

Duly Authorized Officer

Signature: _____

Section 3 Security Responsibilities of Port Facility and Port Operators

3.1   Introduction

3.1.1   This Section provides guidance on the security responsibilities of port facility and port operators under the Maritime Security Measures. Following a general description of the security framework, guidance is offered on:

    a   Security levels;

    b   Security personnel;

    c   Port Facility Security Assessments;

    d   Port Facility Security Plans;

    e   PFSP Implementation;

    f   Statements of Compliance;

    g   Port Security; and

    h   Guidelines for non-SOLAS Marinas, ports and harbours.

3.1.2   Primarily addressed to those responsible for port facility security, the guidance is also relevant to those exercising security responsibilities for the port facility and the Government officials that regulate them.

3.1.3   To facilitate comparisons of the responsibilities of port facility operators with those of Governments and their Designated Authorities, the chart below references the equivalent sub-sections and paragraphs in Section 2.

Port facility operator responsibilities	Maritime Security Measures	Cross-reference to responsibilities for Designated Authorities
3.2.1- 3.2.3	Defining the port facility	2.8.1 - 2.8.12
3.9.3 - 3.9.8	Port Security Committees	2.8.17 - 2.8.18
3.2.5- 3.2.8	Recognized Security Organizations	2.5
3.2.9 - 3.2.10	Alternative Security Agreements	2.13
3.2.11	Equivalent Security Arrangements	2.14
3.3	Changing Security levels	2.6
3.4	Declarations of Security	2.7
3.5.1- 3.5.6	Port Facility Security Officers	2.8.19- 2.8.24
3.6	Port Facility Security Assessments	2.8.25 - 2.8.33
3.7	Port Facility Security Plans	2.8.34 - 2.8.42
3.8.8	Reporting Security Incidents	2.9.38
3.9	Port Security	2.18.16 2.18.20
3.10	Guidelines for Non-SOLAS Marinas, Ports and Harbours	2.18.3 - 2.18.15

3.2   Security Framework

Defining the port facility

3.2.1   In the Maritime Security Measures, a port facility is defined as the location where the ship/port interface occurs. Governments are responsible for identifying which port facilities fall under the Maritime Security Measures and the extent to which they apply to facilities which occasionally serve ships on international voyages. However, port facility operators can assist this process by complying with requests to provide information on the types and frequency of ships using the port facility, their trading patterns, and the cargoes handled, passenger numbers and origins and other security-related information.

3.2.2   Once a port facility has been identified as falling under the Maritime Security Measures, the next step is to establish its geographic boundary. Experience to date indicates that this can be a challenging process due to the need to carefully consider a range of factors including:

a   where passengers embarking and disembark;

b   where dangerous goods or high value cargoes are handled;

c   where containers are loaded, unloaded and stored (both in the short and long term);

d   the economic significance of the port facility;

e   the proximity of the port facility to populated areas;

f   the areas of risk or vulnerability identified by the PFSA;

g   the location of pipelines and related valves (including on the water side);

h   the location of natural barriers (e.g. tree lines, drainage channels and inlets);

i   the location of existing man-made barriers (e.g. fences, walls, roads, access gates).

3.2.3   Experience has also shown that the preparation of a map delineating the area of each port facility should be considered as it can:

a   present the boundary in a way that is clear and easily-understood;

b   show all natural and man-made features which form the boundary or are adjacent to it;

c   be inserted into the PFSA and PFSP;

d   include distances, directions and coordinates; and

e   be easily amended to reflect future changes to the boundary or existing features.

3.2.4   Guidance on preparing a map may be downloaded from the following internet site:
www.infrastructure.gov.au/transport/security/maritime/pdf/GuidancePaperMappingStandardsforPorts.pdf

Recognized Security Organizations

3.2.5   As indicated in sub-section 2.5, Recognized Security Organizations (RSOs) may advise or provide assistance to port facilities on port facility security assessments and plans, including their completion.

3.2.6   Port authorities and port facility operators may be appointed as RSOs provided that they have the appropriate security-related expertise (refer to Appendix 2.3 – Criteria for Selecting Recognized Security Organizations).

3.2.7   RSOs may not approve, verify or certify work products that they have either developed or used sub-contractors to develop.

3.2.8   Experience to date indicates that when a port or port facility operator intends to enter into a contract for the services of a RSO, sound business practice encourages preparation of a formal written agreement signed by both parties. As a minimum, this agreement should:

a   Specify the scope and duration of the work;

b   Identify the main points of contact within the port/port facility and the RSO;

c   Detail the data to be provided to the port administration/port facility operator;

d   Identify the legislation, policies, procedures and other work instruments to be provided to the RSO;

e   Specify the records to be maintained by the RSO and made available as necessary;

      f   Specify any reports to be provided regularly including changes in capability (e.g. loss of key personnel);

      g   Specify a process for resolving performance-related issues.

Alternative Security Agreements

3.2.9   Alternative Security Agreements are agreements between national governments on how to implement the Maritime Security Measures for short international voyages using fixed routes between port facilities within their jurisdiction (sub-section 2.13). To date such agreements usually cover international ferry services and address such topics as acceptance of minor differences in regulatory requirements and security arrangements.

3.2.10   Operators of ports and port facilities covered by such agreements should ensure that they are fully aware of the implications for their operations.

Equivalent Security Arrangements

3.2.11   For port facilities with limited or special operations (e.g. terminals attached to factories or quaysides with occasional operations (sub-section 2.14). It may be appropriate for operators to implement security measures equivalent to those prescribed in the Maritime Security Measures. Details of equivalent security arrangements could be included in the PFSP.

3.3   Changing Security Levels

3.3.1   Governments are responsible for setting security levels and communicating changes rapidly to those who need to be informed including port and port facility operators (sub-section 2.6). This requires Governments, usually through their Designated Authorities, to compile and maintain an accurate set of contact details. In turn, this requires port and port facility operators to promptly communicate changes in contact details.

3.3.2   In addition to having security plans specifying the security measures and procedures in place at each Security level, port and port facility operators should ensure that their plans identify the measures and procedures to be implemented when a ship is operating at a higher security level set by its Administration than that applying at their port or port facility.

3.3.3   Experience to date provides examples of:
      a   For port operators, the PSO being identified as the point of contact;
      b   For port facility operators, the PFSO being identified as the point of contact;
      c   In each case, examples of the manager of the PSO/PFSO being identified as an alternate;
      d   For ports with a PSO, the line of change notification can be a three step 'fan-out' process:
          -   Designated Authority to PSO
          -   PSO to PFSOs and other port stakeholders
          -   PFSOs to key facility personnel and Ship Security Officers (SSOs)
      e   For ports without a PSO, the line of change notification can be a two-step process:
          -   Designated Authority to PFSO(s) and other port stakeholders
          -   PFSOs to key port facility personnel and SSOs
      f   PSOs/PFSOs regularly testing lines of communication;
      g   Multiple means of communicating with contacts i.e. by telephone, e-mail and FAX

3.4   Declarations of Security

3.4.1   A Declaration of Security (DOS) is a written agreement between a port facility and a ship visiting that facility on their respective security responsibilities during the visit (sub-section 2.7). The requirement for a port facility to initiate, complete and retain a DOS is determined by the Designated Authority and includes the conditions under which ships and port facilities may request a DOS.

3.4.2   The Maritime Security Measures contain a model form for a Declaration of Security between a port facility and a ship (refer to Appendix 3.1 – Declaration of Security Form). As well as including information on the identity of the port facility and ship, the form specifies the type of activity to be covered, its duration and the

Security level applying to the particular ship/port interface. If a ship is operating at a higher security level than the port facility the ship/port interface should take place at its higher Security level.

3.4.3   Normally, the DOS is completed by the PFSO. However, if the Designated Authority determines otherwise, it may be handled by another person responsible for shore side security, on behalf of the port facility. When completed, it must be signed and dated both by the PFSO or alternate designated by the Designated Authority and by the ship's Master or ship security officer. Unless there are exceptional circumstances, the DOS only takes effect after it has been signed by both parties in a language common to both parties.

3.4.4   When a ship initiates a DOS, the request shall be acknowledged by the port facility; however, the port facility does not have to comply with the request.

3.4.5   When a port facility initiates a DOS, the request shall be acknowledged by the ship's master or SSO; in this instance, the ship must comply with the request if the ship intends to interface with the port facility.

3.4.6   The conditions under which a DOS may be requested are referenced in paragraph 2.7.3 and should be documented in the PFSP.

3.4.7   The PFSP should detail the procedures to be followed and the security measures and procedures to be implemented when responding to a request for a DOS or initiating a DOS. For a ship/port interface, these could include the respective responsibility accepted by the port facility and ship in accordance with their security plans to:

    a   ensure the performance of all security duties;

    b   monitor restricted areas to ensure that only authorized personnel have access;

    c   control access to the port facility and ship;

    d   monitor the port facility, including berthing areas and areas surrounding the ship;

    e   monitor the ship, including berthing areas and areas surrounding the ship;

    f   handle cargo and unaccompanied baggage;

    g   monitor the delivery of ship's stores;

    h   control the embarkation of persons and their effects;

    i   ensure that security communication is readily available between the ship and port facility.

3.4.8   Experience to date provides examples of:

    a   When the port facility's security measures documented in the DOS are extracted from the PFSP, care being taken to omit sensitive security information such as security standards;

    b   The PFSO notifying the Designated Authority if a ship:

        -   for any reason, refuses a request for a DOS (in addition to denying it entry to the facility;

        -   requesting a DOS is at Security level 3.

    c   The DOS being kept on file for 3 years (which may be longer than the minimum specified by the Designated Authority), so as to be aware of any trends in DOS requests;

    d   At port facilities occasionally used by SOLAS ships, the person ashore responsible for shore-side security (in place of a PFSO), having clear authority to agree a DOS with a SOLAS ship intending to engage in a ship/port interface at the facility.

3.5   Security Personnel

Port Facility Security Officers

3.5.1   Each designated port facility operator is required to appoint a Port Facility Security Officer (PFSO). Refer to paragraphs 2.8.19 to 2.8.24 for more information. Individual PFSOs establish and maintain the security of their port facility and are responsible for maintaining effective contacts with the CSOs and SSOs of ships using their port facility on which efficient operation of the Maritime Security Measures depends.

3.5.2   A PFSO may be responsible for one or more port facilities. Also, it is required to give the PFSO the necessary support to perform the duties listed below including access to required training.

3.5.3   The duties of a PFSO include:

a	Conducting a comprehensive security survey of the port facility, taking into account the approved PFSA;

a   Conducting a comprehensive security survey of the port facility, taking into account the approved PFSA;

b   Ensuring the development and maintenance of the PFSP;

c   Implementing and testing the PFSP;

d   Undertaking regular security inspections of the port facility to ensure that appropriate security measures are in place;

e   Recommending and incorporating, as appropriate, modifications to the PFSP in order to correct deficiencies and take into account relevant changes to the port facility;

f   Enhancing security awareness and vigilance of port facility personnel;

g   Ensuring that adequate training has been provided to personnel responsible for the security of the port facility;

h   Reporting to relevant authorities and maintaining records of incidents which threaten the security of the port facility;

i   Co-ordinating the implementation of the PFSP with appropriate CSOs and SSOs;

j   Co-ordinating with security services, as appropriate;

k   Ensuring that standards for personnel responsible for security of the port facility are met;

l   Ensuring that security equipment is properly operated, tested, calibrated and maintained;

m   Liaising and coordinating appropriate actions with a SSO if advised that:

- a ship is at a higher Security Level than that of the port facility;
- a ship is encountering difficulty in complying with the applicable Maritime Security Measures, including instructions issued by the Contracting Government if the port facility is at Security Level 3; or in implementing the relevant measures and procedures detailed in the SSP;

n   Reporting a ship at a higher Security level than that of the port facility to the competent authority;

o   Assisting SSOs in confirming the identity of those seeking to board ships when requested;

3.5.4   In connection with the last duty identified above, PFSOs should actively seek to facilitate shore leave for ships' crews, crew changes and access of visitors to ships including representatives of seafarers' welfare and labour organizations.

3.5.5   Each person performing the duties of a PFSO should be able to satisfactorily demonstrate the competencies listed in Appendix 3.2 – Competency Matrix for Port Facility Security Officers. Persons who have satisfactorily completed a training course for PFSOs which is recognized by the Designated Authority should be considered to have met this requirement.

3.5.6   Experience to date includes examples of PFSOs and those appointed to undertake their duties:

a   being required to have documentary evidence of their appointment and training;

b   being required to have security clearances, particularly if they have access to sensitive security information provided by the Contracting Government (e.g. information on national threats);

c   being restricted to port facility employees, that is, PFSOs are not contracted in from an external company (e.g. security company or consultancy);

d   having an approved documented list of security and non-security duties (non-security duties should not interfere with the ability to carry out security duties);

e   being active members of port security committees; and

f   reporting to a senior member of the port facility operator's management team.

Other port facility personnel with security-related duties

3.5.7   Other port facility personnel with security-related duties (e.g. guards, access control officers, training officers and relevant port facility managers) are also required to have the knowledge and training required to carry out their assigned duties. They should be able to satisfactorily demonstrate the competencies listed in Appendix 3.3 – Competency Matrix for Port Facility Personnel with Security Duties. Persons who have satisfactorily completed a recognized training course should be considered to have met this requirement.

3.5.8   Experience to date includes examples of other port facility personnel with security-related duties:

  a being required to meet the same or similar requirements as PFSOs (see paragraph 3.5.5 above) with personnel allowed to demonstrate competency by the following alternative means:

    - Having evidence of equivalent service for a period of at least six months in total during the preceding three years; or

    - passing an approved test.

  b before being assigned to their duties, receiving security-related familiarization training, provided by the PFSO or equally qualified person, in their assigned duties in accordance with the provisions specified in the PFSP;

  c being required to have documentary evidence of their training, and;

  d being listed in the PFSP.

All other port facility personnel

3.5.9 All other port facility personnel should receive adequate security-related training so as to contribute collectively to the enhancement of maritime security at the port facility. They should be able to satisfactorily demonstrate the competencies listed in Appendix 3.4 – Competency Matrix for Port Facility Personnel without Security Duties.

3.5.10 Experience to date provides examples of personnel without security-related duties being expected to:

  a receive familiarization training sufficient to enable them to:

    - report a security incident;

    - know the procedures to follow when they recognize a security threat; and

    - take part in security-related emergency and contingency procedures;

  b receive security-related training, provided by the PFSO or equally qualified person, at least once in their career at the port facility, and

  c have documentary evidence of their training.

Security clearances

3.5.11 Port facility operators can be required to comply with any instructions issued by their Government regarding the application of any security clearance procedures for port facility personnel.

3.5.12 Security clearances are the means of verifying that personnel whose duties require access to restricted areas or security sensitive information do not pose a risk to maritime security. The vetting associated with these clearances are more stringent than the pre-employment background checks conducted by port facility operators..

3.5.13 Experience to date includes examples of Governments requiring security clearance for:

  a The senior managers of a port facility;

  b The PFSO and those appointed to undertake the duties of the PFSOs; and

  c In some cases, all those working in any capacity within port areas.

3.6 Port Facility Security Assessments

Introduction

3.6.1 Governments, normally through their Designated Authority, are responsible for carrying out Port Facility Security Assessments (PFSAs) or authorizing RSOs to do so on their behalf (sub-section 2.5).   In practice, the undertaking of PFSAs requires the involvement of port facility operators due to their in-depth knowledge of the port facility's assets, infrastructure, vulnerabilities and past security incidents.

3.6.2 The PFSA may be considered to be a risk analysis of all aspects of a port facility's operations in order to determine which parts of it are more susceptible, and/or more likely, to be vulnerable. It is an essential and integral part of developing or updating the PFSP.

Conducting PFSAs

3.6.3 The PFSA is required to include the following four elements:

<ol type="a" start="1">
a   identification and evaluation of important assets and infrastructure;
b   identification of possible threats to them and the likelihood of their occurrence;
c   identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerabilities; and
d   identification of weaknesses including human factors in the infrastructure, policies and procedures.

3.6.4   A risk assessment and management tool that encompasses these four elements is described in Section 5 along with a list of port security assessment techniques accessible on the internet.

Preparing PFSA Reports

3.6.5   A report shall be prepared upon completion of the PFSA. It provides the means by which a PFSA is approved and is required to:

<ol type="a" start="1">
a   Summarize how the assessment was conducted;
b   Describe each vulnerability found during the assessment;
c   Describe the countermeasures that could address each vulnerability; and
d   Be protected from unauthorized access or disclosure.

3.6.6   As indicated above, the report must be protected from unauthorized access or disclosure. Upon approval, some member states provide a numbered copy to an approved list of individuals within the Designated Authority and port facility and to establish procedures for how the report is to be retained and accessed.

PFSA Coverage of Multiple Facilities

3.6.7   Contracting Governments may allow a PFSA to cover more than one port facility if the operator, location, equipment and design of these port facilities are similar. If such an arrangement is allowed, details must be communicated to the IMO.

3.6.8   Experience to date indicates that no such arrangements have been submitted to the IMO.

Updating PFSAs

3.6.9   PFSAs are to be reviewed and updated periodically or when major changes to the port facility take place (paragraphs 2.8.25 to 2.8.33).

3.6.10   Experience to date includes examples of Designated Authorities producing guidance material recommending that PFSAs should be updated within a short time (e.g. 45 days) after a major change or security incident at the port facility, the term 'major' being used to describe changes to physical structures or operations, or incidents that are sufficient to have an impact on port/port facility operations.

3.6.11   In the absence of any major changes or incidents, PFSAs are reviewed at least every five years, with a shorter period (2-3 years) for larger port facilities.

3.7   Port Facility Security Plans

Introduction

3.7.1   Port Facility Security Plans (PFSPs) shall be developed and maintained based on the results of approved PFSAs conducted at each port facility. The close inter-relationship between PFSAs and PFSPs is shown by the example of a PFSA/PFSP approval process illustrated in Appendix 3.5 – Example of a Port Facility Security Assessment and Plan Approval Process.

3.7.2   PFSPs must be approved by the Designated Authority. RSOs cannot approve them but may assist in their preparation.

3.7.3   PFSPs may be developed by PFSOs or by RSOs acting on their behalf. When RSOs are acting on their behalf, PFSOs continue to be responsible for ensuring that they are properly prepared.

Preparing and Maintaining PFSPs

3.7.4   All PFSPs must provide details of:

a   Measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports, and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;

b   Measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

c   Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;

d   Procedures for responding to any security instructions the Contracting Government in whose territory the port facility is located may give at security level 3;

e   Procedures for evacuation in case of security threats or breaches of security;

f   Duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;

g   Procedures for interfacing with shop security activities;

h   Procedures for the periodic review of the plan and updating;

i   Procedures for reporting security incidents;

j   Identification of the PFSO, including 24-hour contact details;

k   Measures to ensure the security of the information contained in the plan;

l   Measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

m   Procedures for auditing the plan;

n   Procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

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

3.7.5   In addition, PFSPs should detail:

a   The port facility's security organization;

b   The security organization's links with other relevant authorities, the communication systems necessary to allow its effective continuous operation and ships within or approaching the port facility;

c   The basic Security level 1 measures, both operational and physical, that will be in place;

d   The additional security measures that will allow the port facility to progress without delay to Security level 2 and, when necessary, to Security level 3;

e   The procedures for the regular review or audit of the PFSP and for its amendment in response to experience or changing circumstances;

f   The procedures for reporting incidents to the appropriate Contracting Government's contact points; and

g   The procedures for interacting with ships which are operating at a higher Security level set by the ship's Administration than that applying at the port or port facility.

3.7.6   Internet sites which have been developed by member states to illustrate how PFSPs may be prepared and updated are shown in Appendix 3.6 – Examples of Internet Sources of Guidance Material on Preparing, Updating & Implementing Port Facility Security Plans. The Appendix also identifies sources of information on best practices.

3.7.7   Due to conflict of interest considerations, personnel conducting internal audits of the security measures specified in PFSPs or evaluating their implementation are required to be independent of the measures being audited unless this is impracticable due to the size and nature of the port facility.

3.7.8   PFSPs are required to be protected from unauthorized access or disclosure. If PFSPs are kept in electronic format, procedures must be put in place to prevent their unauthorized deletion, destruction or amendment.

3.7.9   Subject to approval by the Designated Authority, a PFSP may cover multiple facilities if their operators, location, type of operation, equipment and design are similar.

3.8   PFSP Implementation

Introduction

3.8.1   Proposed measures in amended PFSPs may not be implemented until authorized by the Designated Authority.

3.8.2   The security measures in PFSPs should be implemented within a reasonable period of their approval. Some member states require PFSPs to specify when proposed measures will be in place and for PFSOs to contact the Designated Authority and discuss contingency plans if there is likely to be any delay.

Planning and Conducting Drills and Exercises

3.8.3   To ensure the effective implementation of PFSPs, drills are required to be carried out on each element at a recommended minimum interval of three months. These are usually organized by PFSOs who are responsible for testing the effective implementation of PFSPs.

3.8.4   To ensure the effective implementation and coordination of PFSPs, PFSOs are required to participate in exercises at a recommended minimum interval of once each calendar year with no more than 18 months between the exercises. These exercises are usually planned and coordinated by port authorities and conducted on a port-wide basis; they may be:

    a   full-scale or live;

    b   tabletop simulation or seminar;

    c   combined with other exercises organized by government agencies or port authorities to test emergency response or commerce resumption plans.

3.8.5   Drills and exercises take up organizational time and resources, and must therefore be conducted in as efficient and effective a manner as possible. Recognizing the need to assist port facility operators in the Asia-Pacific Region, the Asia-Pacific Economic Cooperation (APEC) forum's Transportation Working Group developed a set of guidelines in the form of a manual. It provides a systematic and comprehensive approach to the planning, preparation for, conduct, debrief and reporting of maritime security drills and exercises. Workshops have been delivered to port security officials in several APEC member economies. To provide an appreciation of the scope of these practices, the manual's table of contents is shown in Appendix 3.7 – APEC Manual of Maritime Security Drills & Exercises for Port Facilities: Table of Contents.

3.8.6   The accessible internet site containing the contents of the entire APEC Manual is referenced in Appendix 3.6 – Examples of Internet Sources of Guidance Material on Preparing, Updating & Implementing Port Facility Security Plans.

3.8.7   The conduct of drills and exercises may lead to amendments to the approved PFSP. Major amendments to an approved PFSP should be submitted to the Designated Authority for re-approval.

Reporting Security Incidents

3.8.8   PFSPs are required to document procedures for reporting security incidents and PFSOs are required to report them to relevant authorities.

3.8.9   Security incidents generally fall into two categories:

    a   those considered to be sufficiently serious that they should be reported to relevant authorities by the PFSO including:

        -    unauthorized access to restricted areas within the port facility;

        -    unauthorized carriage or discovery of weapons or prohibited items in the port facility;

        -    incidents of which the media are aware;

        -    bomb warnings;

        -    unauthorized disclosure of a PFSP.

    b   those of a less serious nature but require reporting to, and investigation by, the PFSO including:

        -    breaches of screening points;

        -    inappropriate uses of passes;

- damage to security equipment through sabotage or vandalism;
- suspicious behaviour in or near the port facility;
- suspicious packages in or near the port facility;
- unsecured access points.

3.8.10 Experience to date indicates that some Designated Authorities have:

a specified the types of security incidents that must be immediately reported to them, as indicated below:

Type of security incident
Attack
Bomb warnings
Hijack
Armed robbery against a ship
Discovery of firearms
Discovery of other weapons
Discovery of explosives
Unauthorized access to a restricted area
Unauthorized access to the port facility
Media awareness

b With respect to bomb warnings, developed a checklist as a useful aid for anyone receiving a warning (which can be received in various ways with a telephone call to a port authority, port facility operator or individual ship at the port facility being the most common). One such checklist may be accessed at: www.cpni.gov.uk/Docs/Bomb_threat_checklist.pdf

c designed standard forms for security incidents that must be reported to them and making them available on their internet sites. One such form – the Maritime Security Incident Report Online Form developed by the Australian Government's Department of Infrastructure, Transport, Regional Development and Local Government - may be downloaded from: *www.infrastructure.gov.au/transport/security/maritime/MSIR_online_form.aspx*. Although this form has been designed to fulfil incident reporting requirements prescribed in national legislation, it could be adapted by port facility operators to their particular reporting requirements. In such cases, the form's practical usefulness could be enhanced by:
- Ensuring that its format is straightforward;
- Allowing the PFSO to report the remedial action taken;
- Ensuring that any associated reporting procedures are straightforward;
- Specifying the situations when it is to be forwarded to the port facility's manager; and
- Locating copies where they can be visible to, and easily accessed by, port facility personnel.

Information Security

3.8.11 PFSPs are required to be protected from unauthorized access or disclosure and require the establishment of documented procedures for ensuring the security of information documented in them. Similar requirements apply to PFSAs and other security-sensitive information, including information on cargo movements and cargo.

3.8.12 Experience to date includes examples of Governments providing guidance to port facility operators on:

a ensuring that all sensitive information is password-protected;

b installing access control and security systems in locations where sensitive information is stored (e.g. server rooms and control rooms);

c having effective data back-up procedures.

Shore access for seafarers and on-board visits to ships

3.8.13   The Maritime Security Measures require PFSPs to specify the procedures for facilitating:

      a   shore leave for ship's personnel or personnel changes;

      b   seafarer access to shore-based welfare and medical facilities;

      c   on-board access by visitors including representatives of seafarer's welfare and labour organizations.

3.8.14   In addition to access by visitors to ships, PFSPs should contain procedures at all security levels to cover access by shore-based ship support personnel including those involved with the taking on board of ship's stores and bunkers.

3.8.15   From a practical perspective, it is important that port and port facility operators and security personnel seek a balance between the needs of security and the needs of the ship and its crew. Port facility operators and the port facility security officers should ensure coordination of shore leave for ship personnel or crew change-out, as well as access through the port facility for visitors to the ship, including representatives of seafarers' welfare and labour organizations and those concerned with the maintenance of ships' equipment and safe operation, with the Company in advance of the ship's arrival.

3.8.16   A singular focus on the security of the port facility is contrary to the letter and spirit of Maritime Security Measures and has serious consequences for the international maritime transportation system that is a vital component of the global economy. The ILO/IMO Code of Practice for Port Security also recommends that all port stakeholders work co-operatively to make such arrangements and advance plans.

3.8.17   Port States, while giving effect to security measures to prevent security incidents affecting ships or port facilities and to exercise control over access to their territories, have to recognize that shore leave for seafarers constitutes their right – not a privilege.

3.8.18   Access by authorized personnel to the ship is also a necessity. Wherever practicable, formalities, documentary requirements and procedures should be uniformly applied in order to provide for a consistent application of port facility security measures, provided that such uniformity does not bypass or eliminate the authority of Member States.

3.8.19   PFSOs and PSOs should ensure coordination of these requirements with SSOs, if possible, in advance of the ship's arrival at the port facility. The arrangements should strike a balance between the security needs of ports and port facilities with the needs of the ship and its crew. A single focus on port/port facility security is contrary to the letter and spirit of the Maritime Security Measures.

Conducting Self-Assessments

3.8.20   Checklists provide a useful way to assess and report progress in implementing PFSPs and, by extension, the Maritime Security Measures. Although they can be completed on an as-needed basis, it is a good management practice to conduct such an assessment at least once a year and to establish a link between any identified gaps and work plan priorities. Appendix 3.8 – Implementation Checklist for Port Facility Operators, contains a checklist for port facility operators that can be used to assess progress in implementing the Maritime Security Measures. Except for minor modifications to its format and guidance material, it is identical to the Voluntary Self-Assessment Tool for Port Facility Security that was approved by the IMO's Maritime Safety Committee in May 2006 and received widespread distribution.

3.8.21   PFSOs and PSOs are encouraged to modify the content and format of this checklist in order to ensure that they meet their specific assessment requirements (e.g. to identify when procedures were last reviewed or measures tested).

3.9   Port Security

Introduction

3.9.1   The Maritime Security Measures apply to port facilities. Guidance on wider aspects of port security is contained in the ILO/IMO Code of Practice on Port Security which may be accessed at the following internet site:

www.ilo.org/public/english/dialogue/sector/techmeet/messhp03/messhp-cp-a.pdf. Several Governments have enacted legislation applying parts of the guidance.

3.9.2   There are broad similarities between the guidance offered on port facility security and port security. The significant differences relative to this Section of the Manual are:

  a   Establishing a Port Security Committee;

  b   The appointment of PSOs;

  c   Undertaking Port Security Assessments (PSAs), and

  d   Preparing Port Security Plans (PSPs).

Port Security Committees

3.9.3   At the port level, the development and implementation of security procedures and measures can be enhanced through the establishment of a Port Security Committee (PSC) comprising representatives from the Port/Harbour Authority, the port facilities within the port, government organizations operating in the port, local law enforcement agencies, and those employed in the port as well as port users. Together, those represented on a PSC should have detailed knowledge of the security issues and patterns of criminality experienced at the particular port.

3.9.4   Many port operators have established PSCs to co-ordinate security procedures and measures across their port. Where established, committees have yielded significant security benefits through better co-ordination of security activities across the port and its port facilities.

3.9.5   Membership should be as broad as possible. In addition to the Port Security Officer (PSO)—if appointed—and the PFSO of each facility in the port, it could comprise representatives from the:

  a   management of the port operator and each port facility operator;

  b   Customs and Immigration authorities operating at the port;

  c   law enforcement and emergency services;

  d   port worker associations;

  e   associations for seafarers operating ships from the port;

  f   firms undertaking commercial activities at the port e.g. storage, cargo handling;

  g   shipping companies operating at the port;

  h   shippers/cargo interests at the port;

  i   Designated Authority and Administration assigned to the port;

  j   municipal and regional governments with jurisdictional interests;

  k   community associations adjacent to the port.

3.9.6   Each PSC should have a Terms of Reference which could include:

  a   identifying security threats;

  b   reporting and assessing recent security incidents at the port;

  c   assessing the possible implications of security incidents at other ports;

  d   enhancing co-ordination in the application of security procedures and measures;

  e   planning, coordinating participation in and evaluating security drills and exercises;

  f   coordinating port facility security assessments with the Port Security Assessment;

  g   coordinating, communicating and facilitating the implementation of applicable security measures specified in the Port Security Plan;

  h   facilitating shore leave by seafarers;

  i   sharing best practices and experiences in the implementation of security plans;

  j   designing and evaluating security awareness programs.

3.9.7   Experience to date includes:

  a   The PSC being chaired by the senior manager in the port operator who has overall responsibility for port security (this is usually a position more senior than the PSO);

  b   The PSC appointing a Deputy Chair, usually the PSO, so as to ensure continuity of meetings;

124

c The Terms of Reference being approved by the port operator and available to all interested parties;

d The Terms of Reference specifying the meeting administration responsibilities of the Chair and the meeting participation responsibilities of all members (i.e. to keep their organizations well-informed of proceedings and raise their issues);

e Meetings being held regularly (quarterly is often the minimum frequency – some PSCs meet weekly) so as to enable the timely handling of security matters, with decisions recorded and distributed to all members;

f In order for committees to conduct their business efficiently, consideration being given to limiting attendance to a single representative from each member organization. If necessary, smaller sub-committees could be established to address topics requiring multiple participation from organizations.

3.9.8 There is a need to balance the desired openness of an advisory/consultative committee with the need to protect the confidentiality of sensitive security information (e.g. intelligence on possible threats). In such instances, it may be necessary to establish a special subcommittee restricted to personnel with the necessary security clearances e.g. security officers, police services and government officials.

Port Security Officers

3.9.9 Many port authorities have appointed Port Security Officers (PSOs). Their duties include co-ordination of security activities across the port, including liaison with PFSOs and membership of the Port Security Committee.

3.9.10 At many ports the PSO can be the initial point of contact on security matters with the ships approach the port and intending to use port facilities within the port.

3.9.11 PSOs can also have responsibility for the security of berths operated by the Port Authority or with responsibility for a PFSP which acts as a "master plan" for the port area. They can also have responsibility for the security of anchorages, waiting berths and approaches from seaward under the jurisdiction of the Port Authority.

3.9.12 PSOs can make a significant contribution to the co-ordination of security activities within port areas.

3.9.13 The competencies and training appropriate for PSOs is similar to that for PFSOs. Under the guidance in the ILO/IMO Code of Practice their duties could include:

a Conducting a comprehensive security survey of the port, taking into account the approved PSA;

b Ensuring the development and maintenance of the PSP;

c Implementing and testing the PSP;

d Undertaking regular security inspections of the port to ensure that appropriate measures are in place;

e Recommending and incorporating, as appropriate, modifications to the PSP in order to correct deficiencies and take into account relevant changes to the port;

f Enhancing security awareness and vigilance of port personnel;

g Ensuring that adequate training has been provided to personnel responsible for the security of the port;

h Reporting to the relevant authorities and maintaining records of security incidents that affect the security of the port;

i Coordinating implementation of the PSP with appropriate persons or organizations;

j Coordinating with security services, as appropriate;

k Ensuring that standards for personnel responsible for security of the port are met;

l Ensuring that security equipment is properly operated, tested, calibrated and maintained.

3.9.14 Experience to date provides examples of Governments requiring the appointment of a PSO for each port, including specifying their duties and responsibilities.

3.9.15 Designated Authorities have generally endorsed the appointment of PSOs even when there is no obligation on a Port Authority to do so.

3.9.16 Other examples from experience to date include:

a The appointment of another port officer to undertake the duties of the PSO when necessary;

b   PSOs and other port officers undertaking the duties possessing documentary evidence of their appointment and training;

c   PSOs and other port officers undertaking their duties being port employees, not contracted resources from an external company (e.g. a security firm or consultant);

d   PSOs having an approved documented list of security and non-security duties; non-security duties should not interfere with their ability to carry out their security duties;

e   PSOs playing a key role on Port Security Committees – on occasion acting as Deputy Chair or Secretary; and

f   Ensuring that they report to the senior member of the Port Authority's management team who is the Chair of the Port Security Committee.

Port Security Assessments

3.9.17   Although the Maritime Security Measures do not require port security assessments (PSAs) to be conducted and submitted for approval many Designated Authorities require their port authorities to do so.

3.9.18   The guidance provided on conducting PSAs is similar to the material provided for the conduct and approval of PFSAs.

3.9.19   However, using risk assessment and management tools is much more of a challenge given the larger size of port areas (in some cases with indistinct physical boundaries), the larger scale of potential impacts and vulnerabilities, and the greater number of countermeasures that need to be evaluated.

3.9.20   Experience to date provides examples of Designated Authorities recommending that Port authorities establish a small team to conduct their PSAs . This can help ensure that the key personnel within a port area work together to conduct the assessment. However, given the confidential nature of the information being collated, membership would need to be restricted to those members of the port security committee with appropriate security clearances (e.g. the PSO, PFSOs and their counterparts in national authorities.

Port Security Plans

3.9.21   Although the Maritime Security Measures do not require Port authorities to develop port security plans (PSPs), many do so. Several European States require PSAs and the preparation, submission and approval of PSPs. The guidance available for developing and maintaining PFSPs can be used for PSPs (refer to sub-section 3.7). In instances where PSPs are required to be submitted for approval, PFSPs for facilities within the port area may be attached.

3.9.22   The guidance in sub-section 3.8 on implementing PFSPs can also apply to PSPs.

3.10   Guidelines for Non-SOLAS Marinas, Ports & Harbours

3.10.1   Operators of marinas, ports and harbours which are not required to comply with the Maritime Security Measures may wish to consider taking the following steps:

a   Communicating information to users, such as:
-    the current security environment including parts of the facility which are subject to security conditions and areas of restricted navigation;
-    areas where there might be interaction with SOLAS vessels;
-    any local regulations produced for the guidance and direction of non-SOLAS vessels.

b   If located in a complex of port facilities that are compliant with the Maritime Security Measures, regularly reviewing their security arrangements, in cooperation with the PFSOs.

c   Implementing physical security measures tailored to its size and complexity, such as:
-    adequate illumination;
-    passive monitoring controls and devices;
-    segregation of visiting vessels in one particular area such that the visitors can be effectively monitored;
-    holding transient vessels arriving at night in a specific area, with vessel details recorded;

- installing radio frequency identification device (RFID) or similar systems to monitor the movements of vessels in and out of marinas, ports and harbours.

d   Implementing appropriate security procedures such as training staff to be familiar with security operating procedures for their facility and for the safety of their customers and the public;

e   Implementing regular security patrols, which should include walking all pontoons/docks; checking that boats are moored normally; being alert for any suspicious activity; monitoring access gates, storage shed doors, overhead doors and fuel points; and inspecting restroom facilities.

f   Maintaining a security log of events, which should include:
- details of incidents and events that occurred while on patrol;
- the identity of anyone or any organization called in for emergencies and the time/results of the call;
- details of issues for referral to a supervisor;
- any information which should be noted for the awareness of the next shift personnel.

Appendix 3.1 – Declaration of Security Form

Source: Part B of the ISPS Code

Name of Ship: ....

Port of Registry: ....

IMO Number: ....

Name of Port Facility: ....

This Declaration of Security is valid from …………… until ……………, for the following activities:

(list the activities with relevant details)

under the following security levels:

Security level(s) for the ship: ....

Security level(s) for the port facility: ....

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of the Maritime Security Measures.

Activity	**The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by**	
	The port facility:	**The ship:**
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorised personnel have access		
Controlling access to port facility		
Controlling access to the ship		
Monitoring of port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		

Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of the Maritime Security Measures that will be implemented in accordance with the provisions already stipulated in their approved plans or the specific arrangements agreed to and set out in the attached annex.

Dated at ………………………………… on the …………………………………

Signed for and on behalf of	
the port facility:	the ship:

(Signature of Port Facility Security Officer)   *(Signature of Master or Ship Security Officer)*

Name and title of person who signed	
Name:	Name:
Title:	Title

Contact Details	
(to be completed as appropriate)	
(indicate the telephone numbers or the radio channels or frequencies to be used)	
for the port facility:	for the ship:

Port Facility   Master

....

Port Facility Security Officer   Ship Security Officer

....

                                                 Company

                                                 ....

                                                 Company Security Officer

                                                 ....

Note: This Form is for use between a ship and a port facility. If the Declaration of Security is to cover two or more ships, or a port, this form should be appropriately modified.

Competence • Knowledge Requirements	**Methods for demonstrating competence** • Evaluation Criteria
Develop, maintain and supervise the implementation of a PFSP • International maritime security policy and responsibilities of Governments, Companies and designated persons. • The purpose for and the elements that make up a PFSP, related procedures and maintenance of records. • Procedures to be employed in developing, maintaining and supervising the implementation, and the submission for approval, of a PFSP. • Procedures for the initial and subsequent verification of the port facility's compliance. • Security levels and the consequential security measures and procedures aboard ship and in the port facility environment. • Requirements and procedures for conducting internal audits, on-scene inspections, control and monitoring of security activities specified in a PFSP. • Requirements and procedures for acting upon any deficiencies and non-conformities identified during internal audits, periodic reviews, and security inspections. • Methods and procedures used to modify the PFSP. • Security related contingency plans and the procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship/port interface. • Procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organizations. • Procedures, instructions, and guidance for responding to ship security alerts. • Maritime security terms and definitions (in the Maritime Security Measures).	**Assessment of evidence obtained from approved training or examination.** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Legislative requirements relating to security are correctly identified. • Procedures achieve a state of readiness to respond to changes in security levels. • Communications within the PFSO's area of responsibility are clear and understood.
Assess security risk, threat, and vulnerability • Risk assessment and assessment tools. • Security assessment documentation, including the Declaration of Security. • Techniques used to circumvent security measures. • Enabling recognition, on a non-discriminatory basis, of persons posing potential security risks. • Enabling recognition of weapons, dangerous substances, and devices and awareness of the damage they can cause. • Crowd management and control techniques, where appropriate. • Handling sensitive security related information and security related communications. • Methods for implementing and co-ordinating searches. • Methods for physical searches and non-intrusive inspections.	**Assessment of evidence obtained from approved training or examination** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Procedures achieve a state of readiness to respond to changes in security levels. • Communications within the PFSO's area of responsibility are clear and understood.
Undertake regular inspections of the port facility to ensure that appropriate security measures are implemented and maintained • Requirements for designating and monitoring restricted areas. • Controlling access to the port facility and to restricted areas in the port facility. • Methods for effective monitoring of the port facility and areas surrounding the port facility. • Methods for controlling the embarkation and disembarkation of persons and their effects aboard ships, including the confirmation of identity when requested by the	**Assessment of evidence obtained from approved training or examination.** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Procedures achieve a state of readiness to respond to

Competence	Methods for demonstrating competence
• Knowledge Requirements	• Evaluation Criteria
SSO. • Security aspects relating to the handling of cargo and ship's stores and co-ordinating these aspects with relevant SSOs and CSOs.	changes in security levels. • Communications within the PFSO's area of responsibility are clear and understood.
Ensure that security equipment and systems, if any, are properly operated, tested and calibrated • Various types of security equipment and systems and their limitations. • Methods for testing, calibrating, and maintaining security systems and equipment.	**Assessment of evidence obtained from approved training or examination** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures.
Encourage security awareness and vigilance • Training, drill and exercise requirements under relevant conventions and codes. • Methods for enhancing security awareness and vigilance. • Methods for assessing the effectiveness of drills and exercises. • Instruction techniques for security training and education.	**Assessment of evidence obtained from approved training or examination** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Communications within the PFSO's area of responsibility are clear and understood.

Appendix 3.3 – Competency Matrix for Port Facility Personnel with Security Duties

Source: MSC.1/Circ.1341, May 2010

Competence	Methods for demonstrating competence
• Knowledge Requirements	• Evaluation Criteria
Maintain the conditions set out in a PFSP • Maritime security terms and definitions • International maritime security policy and responsibilities of Governments/Designated Authorities, RSOs, PFSO and designated persons • Maritime security levels and their impact on security measures and procedures in the port facility and aboard ships • Security reporting procedures • Procedures for drills and exercises • Procedures for conducting inspections and surveys and for the control and monitoring of security activities specified in a PFSP • Security-related contingency plans and the procedures for responding to security incidents, including provisions for maintaining critical operations of port facility and ship/port interface • Procedures for handling security-related information and communications • Security documentation including the DOS	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures • Legislative requirements relating to security are correctly identified • Communications within the area of responsibility are clear and understood
Recognition of security threats • Techniques used to circumvent security measures • Enabling recognition of weapons, dangerous substances, dangerous goods, and devices and awareness of damage they can cause • Security-related provisions for dangerous goods • Crowd management and control techniques, where appropriate • Methods for recognition, on a non-discriminatory basis, of patterns which are likely to threaten security	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures and the relevant provisions of the International Maritime Dangerous Goods Code
Inspection, control and monitoring activities • Controlling access to the port facility and its restricted areas • Techniques for monitoring restricted areas • Methods for effective monitoring ship/port interface and areas surrounding the port facility • Inspection methods relating to cargo and stores • Methods for physical searches and non-intrusive inspections	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures and the relevant provisions of the International Maritime Dangerous Goods Code
Proper usage of security equipment and systems • Various types of security equipment and systems, including their limitations • The need for testing, calibrating and maintaining security systems and equipment	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Equipment and systems operations are carried out in accordance with established equipment operating instructions and taking into account the limitations of the equipment and systems • Procedures and actions are in accordance with the principles established by the Maritime Security Measures

Appendix 3.4 – Competency Matrix for Port Facility Personnel without Security Duties

Source: MSC.1/Circ.1341, May 2010

Competence • Basic Knowledge Requirements	Methods for demonstrating competence • Evaluation Criteria
Contribute to the enhancement of maritime security through heightened awareness • Maritime security terms and definitions • International maritime security policy and responsibilities of Government/ Designated Authority, PFSO and designated persons • Maritime security levels and their impact on security measures and procedures in the port facility and aboard ships • Security reporting procedures • Security-related contingency plans • Security-related provisions for dangerous goods	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Requirements relating to enhanced maritime security are correctly identified
Recognition of security threats • Enabling recognition of potential security threats • Techniques used to circumvent security measures • Enabling recognition of weapons, dangerous substances, dangerous goods, and devices and awareness of the damage they can cause • Procedures for security-related communications	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Maritime security threats are correctly identified
Understanding the need for and methods of maintaining security awareness and vigilance • Training, drill and exercise requirements under relevant conventions and codes	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Requirements relating to enhanced maritime security are correctly identified

Appendix 3.5 – Example of a Port Facility Security Assessment and Plan Approval Process
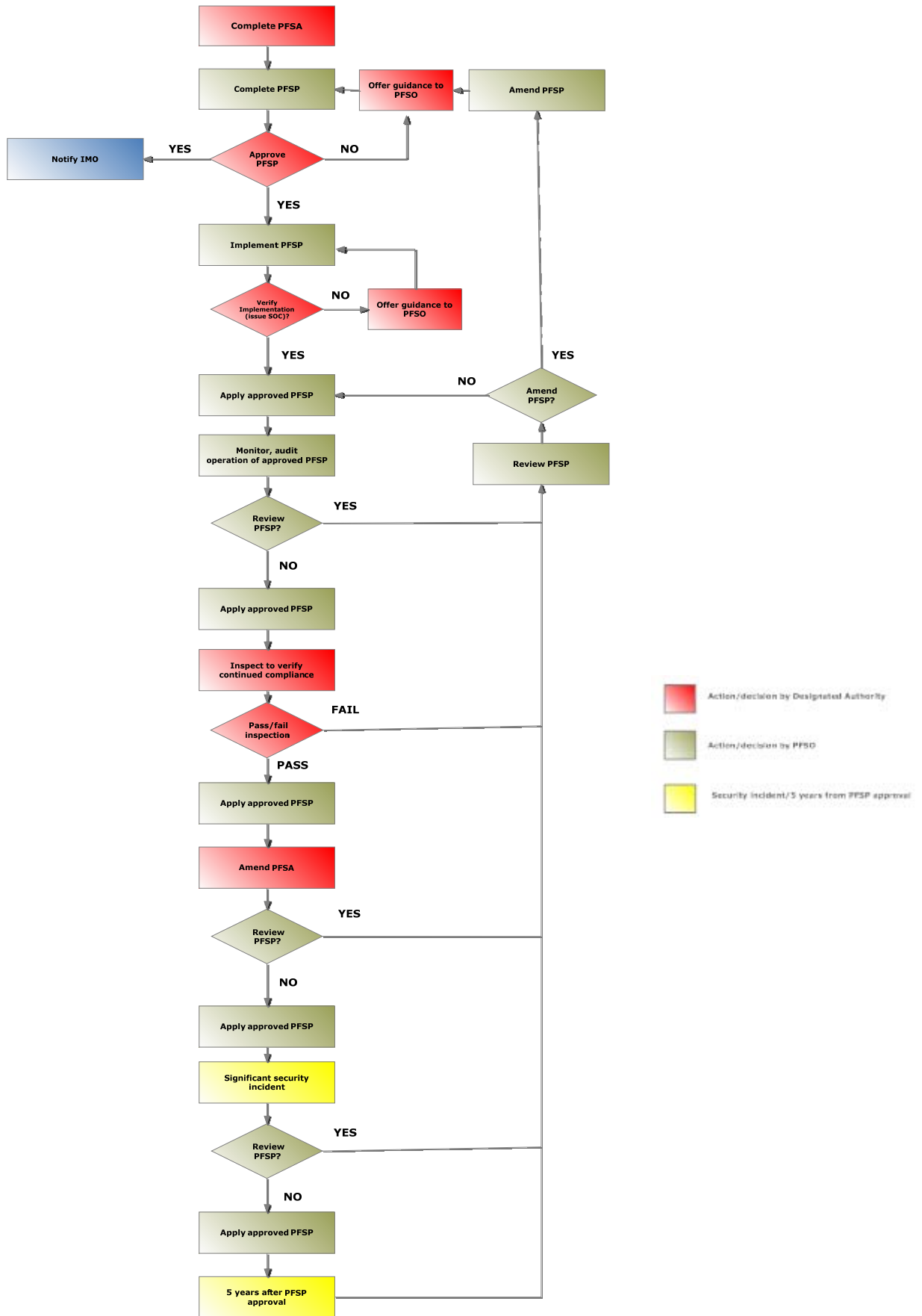
Appendix 3.6 – Examples of Internet Sources of Guidance Material on Preparing, Updating & Implementing Port Facility Security Plans

1.   Australian Government, Department of Infrastructure and Transport: Guide to Preparing a Maritime Security Plan for Port Facility Operators, April 2009. Refer to: www.infrastructure.gov.au/transport/security/maritime

This 33 page guide has been developed to provide port facility operators covered by the Maritime Transport and Offshore Securities Act 2003 with a plan template so as to assist them with meeting all the requirements of an approved plan. It also contains a chart showing the plan approval. Similar guides exist for port operators and port service providers.

2.   United Kingdom, Department for Transport: Port Facility Security Plan, August 2008. Refer to: www.dft.gov.uk/pgr/security/maritime

This 22 page document is a template showing port facility operators how to complete and submit their PFSP.

3.   United States Coast Guard (USCG) Homeport Site. Refer to: www.homeport.uscg.mil

Based on visits to ports in countries trading with the United States, this site documents port security best practices for compliance with the Maritime Security Measures. Its contents have the following characteristics:

- A single page standardised format including description, discussion, potential downside, conclusion, cost and contact information for further details (including the website);

- Emphasis is placed on low cost or innovative practices that are judged to have a significant impact on port facility security;

- The ports listed are generally those where the practice was first observed and the country's national authority has expressed its willingness to share the information;

- The practices are grouped into nine categories:
    - Access Control
    - Documents & Forms
    - Perimeter Control
    - Security Infrastructure
    - Electronic Surveillance
    - Guards & Police
    - Communications
    - Lighting
    - Training & Procedures

APEC's Manual of Maritime Security Drills and Exercises for Port Facilities is included on this site (refer to Appendix 3.7 – APEC Manual of Maritime Security Drills & Exercises for Port Facilities: Table of Contents).

Source: APEC, Transportation Working Group, August 2008 – refer to Item 3 of Appendix 3.7 – APEC Manual of Maritime Security Drills & Exercises for Port Facilities: Table of Contents

Module	Topics Covered
Access Control	Introduction Guidelines for the planning and conduct of maritime security drills Access control drills Person entering without permission Visitor seeking entry without means of identification Person seeking entry using false documents Entry by employees without their security pass Entry by contractor with expired long-term pass Entry by ship crew/shipping agency/seafarer organization representatives without prior notice Vehicle without authorized entry label Vehicle with suspicious person/item Vehicle parked in or in close proximity to a key area or Restricted Area Vehicle forcing entry
Contiguous Zone Security	Introduction Guidelines for the planning and conduct of maritime security drills Contiguous Zone security Persons loitering outside the port facility Person taking photographs of the port facility Person on vessel engaged in suspicious activity Vehicle loitering near the port facility Vessel loitering offshore at the port facility
Materials Handling	Introduction Guidelines for the planning and conduct of maritime security drills Materials handling Suspicious parcel/envelope Suspicious substances Suspicious items Vehicle delivering cargo without proper documents Cargo without proper seals Discovery of unauthorized cargo on board a ship alongside Vehicle delivering ship stores without proper documents Delivery of ship stores without prior notice Unauthorized item found in vehicle delivering ship stores Unauthorized loading/unloading of cargo/ship stores in a restricted area Unaccompanied baggage found in the port facility Unaccompanied baggage found within a Restricted Area Vehicle carrying unaccompanied baggage seeking entry to the port facility
Emergency Response	Introduction Guidelines for the planning and conduct of maritime security drills Emergency response Security surveillance equipment malfunction Perimeter security compromised Activation of intrusion alarm Activation of Ship Security Alert System Power failure Bomb threat Evacuation Changing the Security Level
Ship- Shore Interface	Introduction Guidelines for the planning and conduct of maritime security drills Shore interface Interface with non-ISPS compliant vessel Exchange of Declaration of Security

Principal Exercises	Introduction Guidelines for the planning and conduct of maritime security drills Principal exercises State maritime security exercise Port Facility Security Plan exercise
Port Facility Exercises	Introduction Guidelines for the planning and conduct of maritime security drills Port facility exercise Response to security threats Handling unauthorized items Unauthorized access Cargo and ships' stores Interfacing with ship security activities Security incidents

137

Appendix 3.8 – Implementation Checklist for Port Facility Operators

Source: MSC.1/Circ. 1192, May 2006

This checklist may be used by port facility operators to examine the status of implementation of the Special Measures. The heading of each section is taken directly from paragraph A/14.2 of the ISPS Code.

Completion of the following section is recommended before using the checklist as it can be used to establish an overview of the port facility's operations.

1. Port Facility Overview:

Name of port facility	
Name of operator/authority	
Name of port, if applicable	
Name of PFSO	
Average number of SOLAS ships handled per annum	

2. Particular characteristics of the port facility, if any, including the vessel traffic, which may increase the likelihood of being the target of a security incident:

Passenger ships	☐	Other dangerous goods	☐
Ro-ro/container terminal	☐	Near military installation	☐
Explosives	☐	Military vessels	☐
Oil/gas refinery/terminal	☐	Embarkation of military personnel or cargo	☐
LPG, LNG or petrol storage	☐	Other (describe)	☐

3. Security agreements and arrangements:

Is the port facility covered by an alternative security agreement? If "Yes", provide relevant details.	
Has the port facility implemented any equivalent security arrangements allowed by the Contracting Government? If "Yes", provide relevant details.	
Is the port facility operating under any temporary security measures? If "Yes", have these been approved or authorized by the Contracting Government? If "Yes", provide relevant details.	

Guidance:

- For each question, one of the 'Yes/No/Other' boxes should be ticked. Whichever one is ticked, the 'Comments' box provides space for amplification.
- If the 'Yes' box is ticked, but the measures/procedures are not documented in the PFSP, a short description of them should be included in the 'Comments' box. The 'Yes' box should be ticked only if all procedures or measures are in place. The "comments" box may also be used to indicate when procedures were last reviewed and measures tested (e.g. drills and exercises).
- If the 'No' box is ticked, an explanation of why not should be included in the 'Comments' box along with details of any measures or procedures in place. Suggested actions should be recorded in the 'Recommendations' section at the end of the checklist.

- If the 'Other' box is selected, a short description should be provided in the 'Comments' box (e.g. it could include instances where alternative measures/procedures/agreements or equivalent arrangements have been implemented). If the reason is due to the question not being applicable, then it should be recorded in the 'Comments' box as "not applicable".
- If there is not enough space in the 'Comments' box, the explanation should be continued on a separate page (with the relevant question number and, in the case of questions with multiple options, the option added as a reference).
- The 'Recommendations' boxes at the end of the checklist should be used to record any identified deficiencies and how these could be mitigated. A schedule for their implementation should be included.
- The 'Outcomes' box at the end of the checklist should be used to provide a brief record of the assessment process. Along with the comments in the 'Recommendations' boxes, they form the basis for updating the PFSP.

1. Ensuring the performance of port facility security duties (ISPS Code)

Part A

.1 Does the port facility's means of ensuring the performance of all security duties meet the requirements set out in the PFSP for security level 1 and 2? (ISPS Code, section A/14.2.1)	Yes No Other
Comments:	

.2 Has the port facility established measures to prevent weapons or any other dangerous substances and devices intended for use against persons, ships, or the port, from entering the facility? (ISPS Code, section A/16.3.1)	Yes No Other
Comments:	

.3 Has the port facility established evacuation procedures in case of security threats or breaches of security? (ISPS Code, section A/16.3.5)	Yes No Other
Comments:	

.4 Has the port facility established procedures for response to an activation of a ship security alert system? (ISPS Code, section A/16.3.14)	Yes No Other
Comments:	

Part B – Organization of Port Facility Security Duties (ISPS Code, paragraph B/16.8)

.5 Has the port facility established the role and structure of the security organization? (ISPS Code, paragraph B/16.8.1)	Yes No Other

Comments:	

.6 Has the port facility established the duties and responsibilities for personnel with security roles? (ISPS Code, paragraph B/16.8.2)	Yes No Other
Comments:	

.7 Has the port facility established the training requirements for personnel with security roles? (ISPS Code, sections A18.1, A/18.2, A/18.3 and paragraph B/16.8.2)	Yes No Other
Comments:	

.8 Has the port facility established the performance measures needed to assess the individual effectiveness of personnel with security roles? (ISPS Code, paragraph B/16.8.2)	Yes No Other
Comments:	

.9 Has the port facility established their security organization's link with other national or local authorities with security responsibilities? (ISPS Code, paragraph B/16.8.3)	Yes No Other
Comments:	

.10 Has the port facility established procedures and practices to protect security-sensitive information held in paper or electronic format? (ISPS Code, paragraph B/16.8.6)	Yes No Other
Comments:	

.11 Has the port facility established procedures to assess the continuing effectiveness of security measures and procedures? (ISPS Code, paragraph B/16.8.7)	Yes No Other

Comments:	

.12 Has the port facility established procedures to assess security equipment, to include identification of, and response to, equipment failure or malfunction? (ISPS Code, paragraph B/16.8.7)	Yes No Other
Comments:	

.13 Has the port facility established procedures governing submission and assessment of reports relating to possible breaches of security or security concerns? (ISPS Code, paragraph B/16.8.8)	Yes No Other
Comments:	

.14 Has the port facility established procedures to maintain and update records of dangerous goods and hazardous substances, including their location within the port facility? (ISPS Code, paragraph B/16.8.11)	Yes No Other
Comments:	

.15 Has the port facility established a means of alerting and obtaining the services of waterside patrols and search teams, to include bomb and underwater specialists? (ISPS Code, paragraph B/16.8.12)	Yes No Other
Comments:	

.16 Has the port facility established procedures for assisting, when requested, Ship Security Officers in confirming the identity of those seeking to board the ship? (ISPS Code, paragraph B/16.8.13)	Yes No Other
Comments:	

.17 Has the port facility established the procedures for facilitating shore leave for ship's crew members or personnel changes? (ISPS Code, paragraph B/16.8.14)	Yes No Other

Comments:	

.18 Has the port facility established the procedures for facilitating visitor access to the ship, to include representatives of seafarers' welfare and labour organizations? (ISPS Code, paragraph B/16.8.14)	Yes No Other
Comments:	

2. Controlling access to the port facility (ISPS Code, sections A/14.2.2, A/14.2.1 and A/14.3)

Part A

.1 Does the port facility's means of controlling access to the port facility meet the requirements set out in the PFSP for security level 1 and 2?	Yes No Other
Comments:	

Part B - Establish Facility Security Measures (ISPS Code, paragraphs B/16.10, B16/12, B16/14, B16/17 and B/16.19.1)

.2 Has the port facility identified the appropriate location(s) where security measures can be applied to restrict or prohibit access. These should include all access points identified in the PFSP at security level 1 and 2? (ISPS Code, paragraphs B/16.11, B/16.19.1)	Yes No Other
Comments:	

.3 Does the port facility specify the type of restrictions or prohibitions, and the means of enforcement to be applied at all access points identified in the PFSP at security level 1 and 2? (ISPS Code, paragraphs B/16.11 B/16.19.2, B/16.19.3)	Yes No Other
Comments:	

.4 Has the port facility established measures to increase the frequency of searches of people, personal effects, and vehicles at security level 2? (ISPS Code, paragraph B/16.19.4)	Yes No Other
Comments:	

142

.5 Has the port facility established measures to deny access to visitors who are unable to provide verifiable justification for seeking access to the port facility at security level 2 (ISPS Code, paragraph B/16.19.5)	Yes	No	Other
Comments:			

.6 Has the port facility established the means of identification required to access and remain unchallenged within the port facility? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.7 Does the port facility have the means to differentiate the identification of permanent, temporary, and visiting individuals? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.8 Does the port facility have the means to verify the identity and legitimacy of passenger boarding passes, tickets, etc? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.9 Has the port facility established provisions to ensure that the identification systems are regularly updated? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.10 Has the port facility established provisions to facilitate disciplinary action against those whom abuse the identification system procedures? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.11 Has the port facility created procedures to deny access and report all individuals who are unwilling or unable to establish their identity or purpose for visit to the PFSO and to the national or local authorities? (ISPS Code, paragraph B/16.13)	Yes	No	Other

143

Comments:	

.12 Has the port facility identified a location(s) for searches of persons, personal effects, and vehicles that facilitates continuous operation, regardless of prevailing weather conditions? (ISPS Code, paragraph B/16.14)	Yes No Other
Comments:	

.13 Does the port facility have procedures established to directly transfer persons, personal effects, or vehicles subjected to search to the restricted holding, embarkation, or vehicle loading area? (ISPS Code, paragraph B/16.14)	Yes No Other
Comments:	

.14 Has the port facility established separate locations for embarking and disembarking passengers, ship's personnel, and their effects to ensure that unchecked persons do not come in contact with checked persons? (ISPS Code, paragraph B/16.15)	Yes No Other
Comments:	

.15 Does the PFSP establish the frequency of application of all access controls? (ISPS Code, paragraph B/16.16)	Yes No Other
Comments:	

.16 Does the PFSP establish control points for restricted areas bounded by fencing or other barriers to a standard which is approved by the national government? (ISPS Code, paragraph B/16.17.1)	Yes No Other
Comments:	

.17 Does the PFSP establish the identification of and procedures to control access points not in regular use which should be permanently closed and locked? (ISPS Code, paragraph B/16.17.7)	Yes No Other

Comments:	

3. Monitoring of the port facility, including anchoring and berthing area(s) (ISPS Code sections A/14.2.3 and A/14.3)

Part A

.1 Does the facility's means of monitoring the port facility, including berthing and anchorage area(s) meet the requirements set out in the PFSP for security level 1 and 2?	Yes	No	Other
Comments:			

Part B – Scope of Security Monitoring (ISPS Code, paragraph B/16.49)

.2 Does the port facility have the capability to continuously monitor on land and water the port facility and its nearby approaches? (ISPS Code, paragraph B/16.49)	Yes	No	Other
Comments:			

.3 Which of the following means are employed to monitor the port facility and nearby approaches? (ISPS Code, paragraph B/16.49)	Yes	No	Other
• Patrols by security guards • Patrols by security vehicles • Patrols by watercraft • Automatic intrusion-detection devices • Surveillance equipment	A B C D E		
Comments:			

.4 If automatic intrusion-detection devices are employed, do they activate an audible and/or visual alarm(s) at a location(s) that is continuously monitored? (ISPS Code, paragraph B/16.50)	Yes	No	Other
Comments:			

.5 Does the PFSP establish procedures and equipment needed at each security level? (ISPS Code, paragraph B/16.51)	Yes	No	Other

145

Comments:	

.6 Has the port facility established measures to increase the security measures at security level 1 and 2 (ISPS Code, paragraphs B/16.51, B/16.53.1, B/16.53.2 and B/16.53.3) • Increase intensity and coverage of lighting and surveillance equipment • Increase frequency of foot, vehicle & waterborne patrols • Assign additional personnel • Surveillance	Yes No Other A B C D
Comments:	

.7 Does the PFSP establish procedures and equipment necessary to ensure that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or power disruptions? (ISPS Code, paragraph B/16.51)	Yes No Other
Comments:	

Part B – Illumination at Port Facility (ISPS Code, section A/14.3 and paragraph B/16.49.1)

.8 Does the port facility have adequate illumination, to allow for detection of unauthorized persons at or approaching access points, the perimeter, restricted areas and ships, at all times including the night hours and periods of limited visibility? (ISPS Code, paragraph B/16.49.1)	Yes No Other
Comments:	

4.   Monitoring of restricted areas (ISPS Code, sections A/14.2.4 and A/14.3)

Part A

.1 Does the port facility's means of limiting and monitoring access to restricted areas meet the requirements of the PFSP for security level 1 and 2? (ISPS Code, sections A/14.2.4 and A/14.3)	Yes No Other
Comments:	

Part B – Establishment of Restricted Areas (ISPS Code, paragraph B/16.21)

146

.2 Are restricted areas identified within the port facility? (ISPS Code, paragraph B/16.21)	Yes	No	Other
Comments:			

| .3   Which of the following elements are identified for restricted areas in the PFSP? (ISPS Code, paragraph B/16.21)

• Extent of area
• Times of application
• Security measures to control access to areas
• Security measures to control activities within areas
• Measures to ensure restricted areas are swept before and after establishment

Comments: | Yes   No   Other

A
B
C
D
E |

Part B – Security Measures (ISPS Code, paragraph B/16.22)

.4 Are restricted areas clearly marked, indicating that access to the area is restricted and that unauthorized presence constitutes a breach of security? (ISPS Code, paragraph B/16.23)	Yes	No	Other
Comments:			

.5 Are measures established to control access by individuals to restricted areas? (ISPS Code, paragraph B/16.22.1)	Yes	No	Other
Comments:			

.6 Does the port facility have the means to ensure that passengers do not have unsupervised access to restricted areas? (ISPS Code, paragraph B/16.12)	Yes	No	Other
Comments:			

.7 Are measures established to control the entry, parking, loading, and unloading of vehicles? (ISPS Code, paragraph B/16.22.2)	Yes	No	Other

Comments:	

	Yes No Other
.8 Are measures established to control movement and storage of cargo and ship's stores? (ISPS Code, paragraph B/16.22.3)	Yes No Other
Comments:	

	Yes No Other
.9 Are measures established to control unaccompanied baggage or personal effects? (ISPS Code, paragraph B/16.22.4)	Yes No Other
Comments:	

	Yes No Other
.10 If automatic intrusion-detection devices are installed, do they alert a control centre capable of responding to the alarm? (ISPS Code, paragraph B/16.24)	Yes No Other
Comments:	

	Yes No Other
.11 Which of the following security measures are utilized to control access to restricted areas? (ISPS Code, paragraph B/16.27)	Yes No Other
• Permanent or temporary barriers to surround restricted area	A
• Access points controlled by security guards when in use	B
• Access points that can be locked or barred when not in use	C
• Use of passes to indicate a person's authorization for access	D
• Marking of vehicles that are allowed access	E
• Use of guards and patrols	F
• Use of automatic intrusion-detection devices or surveillance equipment and systems	G
• Control of vessel movement in vicinity of ships using port facility	H
Comments:	

.12 Has the port facility established measures to enhance the security of restricted areas for security level 2? (ISPS Code, paragraph B/16.28)	Yes No Other
• Enhance the effectiveness of barriers	A
• Reduce access points	B
• Enhance control of access points	C
• Restrict parking	D
• Control movement within	E
• Continuously monitor	F
• Enhance frequency of patrols	G
• Limiting access to spaces adjacent to ship	H
Comments:	

.13 Has the port facility established measures to enhance the effectiveness of barriers, reduce access points, and enhance access control for restricted areas at security level 2 (ISPS Code, paragraph B/16.28)	Yes No Other
Comments:	

5.   Supervising the Handling of Cargo (ISPS Code, sections A/14.2.5 and A/14.3)

Part A

.1 Does the port facility's means of supervising the handling of cargo meet the requirements identified in the PFSP for security level 1 and 2?	Yes No Other
Comments:	

Part B - Prevent Tampering, the Acceptance of Unauthorized Cargo, Inventory Control (ISPS Code, paragraph B/16.30.1, B/16.30.2, B/16.31)

.2 Are measures employed to routinely monitor the integrity of cargo, including the checking of seals, upon entry to the port facility and whilst stored in the port facility at security level 1 and 2? (ISPS Code, paragraph B/16.32.1)	Yes No Other
Comments:	

.3 Are measures employed to routinely monitor cargo transport units prior to and during cargo handling operations? (ISPS Code, paragraph B/16.32.1)	Yes No Other
Comments:	

149

.4 Which of the following means are employed to conduct cargo checking? (ISPS Code, paragraph B/16.33)	Yes No Other
• Visual exam • Physical exam • Scanning or detection equipment • Other mechanical means • Dogs	A B C D E
Comments:	

.5 Are restricted areas designated to perform inspections of cargo transport units if a container seal appears to have been compromised? (ISPS Code, paragraph B/16.32.4)	Yes No Other
Comments:	

.6 Has the port facility established measures to intensity checks to ensure that only documented cargo enters the facility, and if necessary, is only stored on a temporary basis at security level 2? (ISPS Code, paragraph B/16.35.2)	Yes No Other
Comments:	

.7 Has the port facility established measures to intensify vehicle searches, the frequency and detail of examining cargo seals, and other tampering prevention methods at security level 2? (ISPS Code, paragraph B/16.35.3)	Yes No Other
Comments:	

.8 Are cargo delivery orders or equivalent cargo documentation verified before acceptance? (ISPS Code, paragraph B/16.32.2)	Yes No Other
Comments:	

.9 Are procedures utilized to randomly or selectively search vehicles at facility access points? (ISPS Code, paragraph B/16.32.3)	Yes	No	Other
Comments:			

.10 Are inventory control procedures employed at facility access points? (ISPS Code, paragraph B/16.31)	Yes	No	Other
Comments:			

.11 Are means of identification used to determine whether cargo inside the port facility awaiting loading has been either checked and accepted or temporarily stored in a restricted area? (ISPS Code, paragraph B/16.31)	Yes	No	Other
Comments:			

6.   Supervising the handling of ship's stores (ISPS Code, sections A/14.2.6 and A/14.3)

Part A

.1 Does the port facility's means of supervising the handling of ship's stores meet the requirements identified in the PFSP at security level 1 and 2? (ISPS Code, section A/14.2.6)	Yes	No	Other
Comments:			

Part B – Ship's Stores Security Measures (ISPS Code, paragraph B/16.38)

.2 Are ship's stores examined to ensure package integrity at security level 1 and 2? (ISPS Code, paragraphs B/16.38.1 and B/16.42.1)	Yes	No	Other
Comments:			

.3 Are procedures established to ensure that no ship's stores are accepted into the port facility without checking at security level 1 and 2? (ISPS Code, paragraphs B/16.38.2 and B/16.42.2)	Yes	No	Other

151

Comments:	

	Yes No Other
.4 Which of the following means are employed to inspect ship's stores? (ISPS Code, paragraph B/16.41) • Visual exam • Physical exam • Scanning or detection equipment • Other mechanical means • Dogs Comments:	A B C D E

	Yes No Other
.5 Are procedures established to prevent the tampering of ship's stores? (ISPS Code, paragraph B/16.38.3) Comments:	

	Yes No Other
.6 Are ship's stores deliveries preceded with an advanced notification of load composition, driver information, and vehicle registration? (ISPS Code, paragraph B/16.40.2) Comments:	

	Yes No Other
.7 Are unscheduled deliveries of ship's stores declined access to the port facility? (ISPS Code, paragraph B/16.38.4) Comments:	

	Yes No Other
.8 Are there procedures in place to prevent ships' stores being accepted unless ordered? Are manifests and order documentation validated prior to allowing then into the port facility at security level 1 and 2? (ISPS Code, paragraph B/16.38.4) Comments:	

152

.9 Are searches of vehicles delivering ship's stores performed prior to entry into the port facility? (ISPS Code, paragraph B/16.38.5)	Yes	No	Other
Comments:			

.10 Are escorts provided for ship's stores delivery vehicles within the port facility at security level 1 and 2? (ISPS Code, paragraphs B/16.38.6 and B/16.42.4)	Yes	No	Other
Comments:			

.11 Does the port facility increase the use of scanning/detection equipment mechanical devices, or dogs at security level 2? (ISPS Code, paragraph B/16.43.2)	Yes	No	Other
Comments:			

7.   Ensuring security communication is readily available (ISPS Code, sections A/14.2.7 and A/14.3)

Part A

.1 Do the port facility's communication equipment and procedures meet the requirements identified in the PFSP at security level 1 and 2? (ISPS Code, section A/14.2.7)	Yes	No	Other
Comments:			

Part B – Effectiveness and protection of Communication Equipment, Procedures and Facilities (ISPS Code, paragraph B/16.8.4 and B/16.8.5)

.2 Is the port facility equipped with auxiliary communication systems for both internal and external communications that are readily available regardless of security level, weather conditions or power disruptions at security level 1 and 2? (ISPS Code, paragraph B/16.8.4)	Yes	No	Other
Comments:			

.3 Are security personnel trained on communication equipment to ensure efficiency? (ISPS Code, paragraph B/16.8.4)	Yes	No	Other

Comments:	

.4 Are telephone numbers for key personnel accurate and routinely validated? (ISPS Code, paragraph B/16.8.4)	Yes No Other
Comments:	

.5 Are procedures in place to ensure that port facility communication systems and equipment are serviced and maintained? (ISPS Code, paragraph B/16.8.4)	Yes No Other
Comments:	

.6 Has the port facility established procedures and means for the PFSO to effectively disseminate changes in the security level at the port facility or with a vessel interfacing with the port? (ISPS Code, paragraph B/16.8.4)	Yes No Other
Comments:	

.7 Are security procedures established to protect radio, telecommunication equipment and infrastructure, and computer systems? (ISPS Code, paragraph B/16.8.5)	Yes No Other
Comments:	

.8 Are entry control procedures established to restrict access of communication facilities and infrastructure? (ISPS Code, paragraph B/16.8.5)	Yes No Other
Comments:	

8. Training, Drills and Exercises (ISPS Code section A/18)

Part A

.1 Has the PFSO and appropriate port facility security personnel received sufficient training to perform their assigned duties as identified in the PFSP? (ISPS Code, sections A/18.1 and A/18.2)	Yes	No	Other
Comments:			

.2 Has the port facility implemented drills and exercises? (ISPS Code, sections A/18.3 and A/18.4)	Yes	No	Other
Comments:			

Part B – Training, drills, and exercises on port facility security (paragraphs B/18.1, B/18.2, B/18.3, and B/18.6)

.3 Are the PFSO, personnel with security duties and all other port facility personnel familiar with the relevant provisions of the PFSP and have they received the appropriate levels of training? (paragraphs B/18.1, B/18.2 and B/18.3)	Yes	No	Other
Comments:			

.4 Are security drills conducted at least every three months and security exercises conducted at least once each calendar year with no more than 18 months between the exercises? (ISPS Code, paragraphs B/18.5 and B/18.6)	Yes	No	Other
Comments:			

9. Miscellaneous

.1 Has the port facility established procedures and adopted measures with respect to ships operating at a higher security level than the port facility? (ISPS Code, paragraph B/16.55)	Yes	No	Other
Comments:			

.2 Has the port facility established procedures and adopted measures which can be applied when it is interfacing with (ISPS Code, paragraph 16.56): • a ship which has been at a port of a State which is not a Contracting Government • a ship to which the ISPS Code does not apply • service vessels covered by the PFSP are interfacing with fixed or floating platforms or mobile offshore drilling units on location	Yes No Other A B C
Comments:	

Recommendations

This section should be used to record any deficiencies identified by the checklist and how these could be mitigated. In essence, it provides an action plan for the PFSO.

Recommendations/For Action: Section 1: Ensuring the performance of port security duties.

....
....

Recommendations/For Action: Section 2: Controlling access to the port facility.

....
....

Recommendations/For Action: Section 3: Monitoring of the port facility, including anchoring and berthing areas.

....
....

Recommendations/For Action: Section 4: Monitoring of restricted areas.

....
....

Recommendations/For Action: Section 5: Supervising the handling of cargo.

....
....

Recommendations/For Action: Section 6: Supervising the handling of ships' stores.

....
....

Recommendations/For Action: Section 7: Ensuring security communication is readily available.

....
....

Recommendations/For Action: Section 8: Training, drills and exercises.

....
....

OUTCOMES

This section should be used by the port facility operator to record findings any other issues arising. These could be raised with port facility staff or be used as the basis to seek guidance from the Designated Authority, as appropriate.

Signature of assessor	Date of completion
Name	Title
…………………………………......	……………………..................................

Section 4 Security Responsibilities of Ship Operators

4.1   Introduction

4.1.1   This Section provides guidance on the responsibilities of ship operators under the Maritime Security Measures. Following a general description of the security framework, guidance is offered on:

    a   Security levels;

    b   Ship security personnel;

    c   Ship security communications;

    d   Ship Security Assessments;

    e   Ship Security Plans;

    f   Security-related documentation and information, and

    g   Guidelines for Non-SOLAS vessels.

4.1.2   Primarily addressed to those undertaking ship security responsibilities, the guidance is also relevant for those responsible for the security of the port facilities with which ships interface and for Government officials with regulatory responsibilities for shipping activities.

4.1.3   The Maritime Security Measures specify the responsibilities of Governments and, to a lesser extent, those of ship operators. To facilitate comparisons of the responsibilities of ship operators with those of Governments and their Administrations, the chart below references the equivalent Sections and paragraphs in Section 2.

Ship operator responsibilities	Maritime Security Measure	Cross-reference to responsibilities for Administrations
4.2.5	Participation on Port Security Committees	2.8.17 - 2.8.18
4.2.6 - 4.2.8	Recognized Security Organizations	2.5
4.2.10 - 4.2.11	Alternative Security Agreements	2.13
4.2.12	Equivalent Security Arrangements	2.14
4.3	Changing Security levels	2.6
4.4	Declarations of Security	2.7
4.5	Ship security personnel	2.9.1 - 2.9.11
4.6.1 - 4.6.10	Ship Security Alert Systems	2.12.4 - 2.12.15
4.6.11 - 4.6.12	Automatic identification systems	2.12.16 - 2.12.19
4.6.13 - 4.6.15	Pre-Arrival information	2.12.20 - 2.12.24
4.6.16 - 4.6.18	Long-range Identification & Tracking systems	2.12.25 - 2.12.37
4.7	Ship Security Assessments	2.9.12 - 2.9.14
4.8.1 - 4.8.11	Ship Security Plans	2.9.15 - 2.9.29
4.8.30- 4.8.33	Shore leave and access to shore-based facilities by seafarers	2.17.6 - 2.17.10
4.8.34 - 4.8.37	Reporting Security Incidents	2.9.36
4.8.38 - 4.8.39	Maintaining On-board Records	2.9.37
4.9	International Ship Security Certificates	2.10
4.10.1 - 4.10.7	Control and Compliance Measures	2.11
4.11	Guidelines for non-SOLAS Vessels	2.18.3 - 2.18.15

4.2   Security Framework

Extent of Application of Maritime Security Measures

4.2.1   Ships falling under the Maritime Security Measures may be grouped into the following categories:

a   *Passenger ships*, including high-speed passenger craft, carrying 12 or more passengers;

b   *Cargo ships* of 500 gross tonnage and upwards, including high-speed craft, bulk carriers, chemical tankers, gas carriers and oil tankers;

c   *Mobile offshore drilling units*, which are vessels capable of drilling for resources beneath the sea-bed. The Maritime Security Measures are only applicable when they are underway. When they are on site on the Continental Shelf, they are subject to any security requirements that the coastal State applies to its offshore activities;

d   *Special purpose ships* over 500 gross tons that are not Government-owned and that, by reason of their functions, carry on board more than 12 personnel other than normal crew who are engaged in special duties. These include research and survey ships, training ships, fish processing and factory ships, salvage ships, cable and pipe laying ships, diving ships and floating cranes.

4.2.2   The Maritime Security Measures do not apply to ships engaged in domestic voyages or the following types of ships engaged in international voyages:

a   warships, naval auxiliaries or other ships operated by a Government and used only on Government non-commercial business;

b   cargo ships of less than 500 gross tons;

c   ships not propelled by mechanical means;

d   wooden ships of primitive build;

e   pleasure vessels not engaged in trade; or

f   fishing vessels.

4.2.3   Experience to date indicates that some Administrations:

a   Have not fully applied the Maritime Security Measures to traditional sailing vessels although they fall into the category of Special Purpose Ships;

b   Exempted ships that are not normally engaged as Special Purpose Ships but undertake an exceptional single special purpose voyage (provided that they comply with the safety requirements judged to be adequate for the voyage by the Administration).

c   Using risk-based assessments, have extended the application of the Maritime Security Measures to certain categories of non-SOLAS vessels such as ferries operating domestic services; and

d   are actively encouraging non-SOLAS vessel owners and operators to voluntarily apply some of the basic security practices and principles contained in the Maritime Security Measures as it helps to strengthen the overall maritime security framework (refer to sub-section 4.10).

Overview of Shipping Company Responsibilities

4.2.4   Shipping companies are required to ensure that:

a   Each ship security plan clearly states the master's overriding authority to:
  -    make decisions with respect to the safety and security of the ship;
  -    request assistance from the company or Governments as may be necessary.

b   CSOs, ships' masters and their SSOs are given the necessary support to fulfill their duties and responsibilities.

c   For each ship, a security assessment is conducted and its documentation retained.

d   Masters have information on board that allows authorized government officials to establish:
  -    who is responsible for appointing crew members or other persons on-board their ship to duties on the ship;
  -    who is responsible for deciding the employment of the ship;
  -    who are the parties to any charter that the ship is employed under.

Participation on Port Security Committees

4.2.5   There is no requirement for shipping companies to participate on port security committees. However there can be advantages if companies are represented particularly on the Committees at their home port or other ports used frequently by their ships. Active participation helps to ensure that key aspects of the ship-shore interface such as shore leave for crew members and access to ships can be effectively dealt with. Guidance on Port Security Committees is in paragraphs **Error! Reference source not found.** to **Error! Reference source not found.**.

Recognized Security Organizations

4.2.6   Administrations may authorize Recognized Security Organizations (RSOs) to act on their behalf (refer to sub-section 2.5) to:

      a   approve SSPs;

      b   verify and certify compliance of ships with the provisions of the Maritime Security Measures.

4.2.7   Shipping companies may use RSOs or experts from other organizations to provide advice and assistance on SSAs and SSPs. However, RSOs should not approve SSPs if they have been involved in their preparation or the conduct of the related SSAs.

4.2.8   Experience to date includes examples of shipping companies contracting the services of a RSO having a formal written agreement signed by both parties that, as a minimum:

      a   specifies the scope and duration of the work;

      b   identifies the main points of contact in both the company and the RSO;

      c   details the data to be provided to the company;

      d   identifies the legislation, policies, procedures and other work instruments to be provided to the RSO;

      e   specifies the records to be maintained by the RSO and made available as necessary;

      f   specifies any reports to be provided regularly including changes in capability (e.g. loss of key personnel), and

      g   specifies a process for resolving performance-related issues.

Alternative Security Agreements

4.2.9   Alternative Security Agreements are agreements between national governments on how to implement the Maritime Security Measures for short international voyages (refer to definition in paragraph 1.8.1eee) using fixed routes between port facilities within their jurisdiction (refer to sub-section 2.13). The majority of such agreements cover international ferry services and may address such topics as:

      a   Acceptance of minor differences in regulatory requirements;

      b   Alternative security arrangements to those in the Maritime Security Measures;

      c   A single security assessment for all ships covered by the agreement;

      d   How Declarations of Security are to be handled;

      e   How pre-arrival information is to be handled.

4.2.10   Ships covered by an Alternative Security Agreement cannot conduct any ship-to-ship activities with ships not covered by that Agreement.

4.2.11   Experience to date indicates that CSOs have actively participated in the security assessments and negotiations leading to the adoption of Alternative Security Agreements.

Equivalent Security Arrangements

4.2.12   An Administration may allow a ship or group of ships entitled to fly its flag to implement security measures equivalent to those prescribed in the Maritime security measures (refer to sub-section 2.14). Equivalent security arrangements could be included in the SSP.

4.3   Changing Security Levels

4.3.1   Governments are responsible for setting security levels and communicating changes rapidly to those who need to be informed including shipping companies (refer to sub-section 2.6). This requires governments, through their Administrations, to compile and maintain an accurate set of contact details. In turn, this requires shipping companies to promptly communicate changes in contact details.

4.3.2   Ships intending to enter a port or port facility usually establish the Security level applying at the port or port facility through direct contact with the port authority, or the port or port facility security officer, prior to entry.   If a ship is operating at a higher security level than that applying at the port or port facility, the information should be passed to the port authority or the port or port facility security officer prior to entry.

4.3.3   A ship can never operate at a lower Security level than the one being applied at the port or port facility that it is visiting.

4.3.4   A ship can, however, operate at a higher security level, when set by their Government, than that applying at the port or port facility it is in, or it intends to enter. The authorities at the port/port facility should not seek to have the ship reduce the security level set by the ship's Government.

4.3.5   If Governments have set higher security levels to a ship using a foreign port or port facility entry procedures can be simplified if the decision is also communicated Government-to-Government.

4.3.6   In addition to security plans specifying the security measures in place at each Security level, ship operators should ensure that their plans identify the measures and procedures to be implemented when their ships are operating at a higher security level set by its Administration than that applying at the port or port facility which they are seeking to enter.

4.3.7   Experience to date includes examples of:
  a   CSOs being appointed as the point of contact for shipping companies;
  b   The appointment of a senior manager within the shipping company as an alternative contact point;
  c   The line of change notification being a two-step process:
    -    Administration to CSOs
    -    CSOs to key company personnel and SSOs
  d   CSOs regularly testing lines of communication, and
  e   Multiple means of communicating with contacts i.e. by telephone, e-mail and FAX

4.4   Declarations of Security

4.4.1   The requirement for a ship to initiate, complete and retain a Declaration of Security (DOS) is determined by the ship's Administration (refer to sub-section 2.7).

4.4.2   Details of how a port facility initiates or responds to a request for a DOS with a ship is documented in sub-section 3.4. The Maritime Security Measures contain a model form for a DOS between a ship and a port facility (refer to Appendix 3.1 – Declaration of Security Form).

4.4.3   This model DOS form can be modified for a DOS between ships, as provided in Appendix 4.1 – Sample of a Declaration of Security Form for a Ship-to-Ship Interface. As well as including information on the name, port of registry and IMO number of both ships, the DOS should specify the types of activity it covers, its duration and the Security level applying to both ships. The activity should take place at the higher Security level if the ships are operating at different security levels.

4.4.4   Normally, the DOS is completed by the ship's master or the SSO acting on his behalf. When completed, it must be signed and dated both by the ship's Master or SSO and, in the case of a ship/port interface, by the PFSO (or alternate designated by the Designated Authority). In the case of ship-to-ship activity, it must be signed and dated by both Masters or their SSOs. Unless there are exceptional circumstances, the DOS only takes effect after it has been signed by both parties in a language common to both parties.

4.4.5   When a ship initiates a DOS, the port facility is required to acknowledge the request; however, it does not have to comply with the request.

4.4.6   When a port facility initiates a DOS, the request shall be acknowledged by the ship's master or SSO and the ship must comply with the request if the ship intends to continue its interface with the port facility.

4.4.7   The conditions under which a DOS may be requested are documented in paragraph 2.7.3. Those relevant to ships should be documented in the SSP.

4.4.8   The SSP should detail the procedures to be followed and the security measures and procedures to be implemented when responding to a request for a DOS or initiating a DOS. For a ship/port interface, these could include the respective responsibility accepted by the port facility and ship in accordance with their security plans to:

     a   ensure the performance of all security duties;

     b   monitor restricted areas to ensure that only authorized personnel have access;

     c   control access to the port facility and ship;

     d   monitor the port facility, including berthing areas and areas surrounding the ship;

     e   monitor the ship, including berthing areas and areas surrounding the ship;

     f   handle cargo and unaccompanied baggage;

     g   monitor the delivery of ship's stores;

     h   control the embarkation of persons and their effects;

     i   ensure that security communication is readily available between the ship and port facility.

4.4.9   For a ship-to-ship activity, the respective responsibility accepted by each ship in accordance with its SSP is the same as above except that 'port facility' is replaced by 'ship'.

4.4.10   When a SSO on a SOLAS ship is unable to contact a person ashore with responsibility for shore-side security including completion of a DOS, the SSO can prepare a DOS indicating the security measures and procedures to be applied and maintained by the ship for the duration of the ship/port interface.

4.4.11   A SOLAS ship intending to undertake ship-to-ship activities with a non-SOLAS ship is normally required to complete a DOS with the non-SOLAS ship. Since the Maritime Security Measures were introduced, non-SOLAS ships have become accustomed to responding positively to such requests. If a DOS cannot be agreed between a SOLAS ship and a non-SOLAS ship, it is unlikely that ship-to-ship activity should take place.

4.4.12   Experience to date includes examples of:

     a   When the ship's security measures documented in the DOS are extracted from the SSP, care being taken to omit sensitive security information such as security standards;

     b   The SSO notifying the Designated Authority if a port facility:

         -   for any reason, refuses a request for a DOS

         -   requesting a DOS is at Security level 3.

     c   The DOS being kept on file for 3 years (which may be longer than the minimum specified by the Administrations), so as to be aware of any trends in DOS requests; and

     d   SSPs including a requirement for ships to seek agreement of a DOS when using such a non-SOLAS port facility.

4.5   Ship security personnel

Introduction

4.5.1   This section provides guidance on the duties and security-related training required for Company Security Officers (CSOs), Ship Security Officers (SSOs) and all shipboard personnel (refer to paragraph 1.8.1uu for the definition). Related guidance is in paragraphs 2.9.1-11.

4.5.2   The appointment of CSOs and SSOs is essentially a matter for the shipping company whose ships fall under the Maritime Security Measures.

4.5.3   As the CSOs and SSOs are likely to be entrusted with security-sensitive information, some Administrations require that they are subjected to security vetting before receiving such information. This requirement can extend to other company personnel who perform the responsibilities of a CSO and to the senior management of the company.

4.5.4   Certificates of proficiency issued by the ship's Administration to SSOs and shipboard personnel under the STCW Code can be one of the documents inspected by a duly authorized officer undertaking control and compliance measures under the Maritime Security Measures when the ship is in a foreign port (refer to paragraphs 4.10.1-7).

Company Security Officers

4.5.5   In shipping companies, the responsibility for the security of a ship rests with the CSO. Working together with their SSOs and with the PFSOs at the port facilities used by their ships, CSOs play a central, and essential, role in the implementation of the Maritime Security Measures. It is their responsibility to ensure that each of their ships meets the requirements of the Maritime Security Measures.

4.5.6   On security matters, they are the main point of contact with both their ships and the Administration CSOs can be the officers within companies who are directly notified of changes in Security level for onward transmission to their ships.

4.5.7   Through their contact with their SSOs and PFSOs, they can ensure:
   a   that possible security threats are identified and appropriate action taken to address them; and
   b   the continued effectiveness of the security measures and procedures on their ships.

4.5.8   Each shipping company is required to appoint one or more CSOs. The ship or ships that each CSO is responsible for should be clearly identified.

4.5.9   The duties of a CSO include:
   a   Advising on the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
   b   Ensuring that ship security assessments are carried out;
   c   Ensuring the development, submission for approval, implementation and maintenance of ship security plans;
   d   Ensuring that ship security plans are modified, as appropriate, to correct deficiencies and satisfy the security requirements of individual ships;
   e   Arranging for internal audits and reviews of security activities;
   f   Arranging for the initial and subsequent verifications of ships by the Administration or RSOs authorized to act on their behalf;
   g   Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly dealt with;
   h   Enhancing security awareness and vigilance;
   i   Ensuring adequate training for personnel responsible for ship security;
   j   Ensuring effective communication and co-operation between SSOs and relevant PFSOs;
   k   Ensuring consistency between security requirements and safety requirements;
   l   Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately;
   m   Ensuring that any alternative or equivalent security arrangements approved for a particular ship or group of ships are implemented and maintained; and
   n   Ensuring the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals.

4.5.10   Each person performing the duties of a CSO should be able to satisfactorily demonstrate the competencies listed in Appendix 4.2 – Competency Matrix for Company Security Officers. Persons who

have satisfactorily completed a training course for CSOs which is recognized by the Administration should be considered to have met this requirement.

4.5.11   As CSOs are not serving on board ships they do not fall under the provisions of the STCW Convention and its related Code.

4.5.12   Other shore-based personnel with security responsibilities are required to be able to demonstrate the same competencies.

4.5.13   Some of the practices observed in the appointment and certification of CSOs include:

    a   having to undergo an approval process based on training course certification and security clearances, particularly if they have access to sensitive security information provided by the Contracting Government (e.g. information on national threats);

    b   having to attend courses from training organizations approved by their Administration;

    c   designating an alternate to undertake the duties of the CSO when necessary;

    d   having documentary evidence of their appointment and training (this includes their alternate);

    e   being shipping company employees and not contracted from an external company such as a security firm or consultant (this includes their alternate);

    f   having an approved list of their security and non-security duties. Non- security duties should not interfere with their ability to carry out their security duties;

    g   wherever possible, being members of Port Security Committee at their home port, and

    h   reporting directly to a senior member of the shipping company's management team;

Ship Security Officers

4.5.14   On a ship, the Ship Security Officer (SSO) is responsible for security. This responsibility gives SSOs a key role in ensuring the continued effectiveness of the Maritime Security Measures.

4.5.15   Responsible to the master of their ship and reporting to the CSOs ashore, SSOs:

    a   ensure that the ship and its shipboard personnel operate in accordance with the approved SSP;

    b   maintain security at all times;

    c   may have responsibility for shipboard personnel with designated security responsibilities;

    d   ensure that contact is established and maintained with the PFSOs at the port facilities that the ship uses; and

    e   liaise as necessary with PSOs/PFSOs or other officers and officials ashore with security responsibilities.

4.5.16   A SSO must be designated for every SOLAS ship. To allow for crew changes a number of SSOs may be designated to serve on each ship.

4.5.17   The duties of a SSO include:

    a   Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

    b   Maintaining and supervising the implementation of the SSP, including any amendments;

    c   Co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and relevant PFSOs;

    d   Proposing modifications to the SSP;

    e   Reporting any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance to the CSO;

    f   Implementing any corrective actions;

    g   Enhancing security awareness and vigilance on-board the ship;

    h   Ensuring that adequate training has been provided to shipboard personnel, including security-related familiarization training;

    i   Reporting all security incidents;

j   Co-ordinating implementation of the SSP with the CSO and relevant PFSOs;

k   Ensuring that security equipment is properly operated, tested, calibrated and maintained; and

l   Ensuring the effective implementation of the SSP by organizing drills at appropriate intervals.

4.5.18   Effective January 1, 2012, SSOs are required to hold a certificate of proficiency confirming that they:

a   have approved seagoing service of not less than 12 months (or appropriate seagoing service and knowledge of ship operations); and

b   meet the minimum standards of competency specified in the STCW Code, which are listed in Appendix 4.3 – Competency Matrix for Ship Security Officers. They are similar to the guidance issued by the IMO for CSOs in 2005 (refer to Appendix 2.4 – Sample of a Port Facility Security Plan Approval Form).

4.5.19   The 2006 amendments to the STCW Convention which came into force in 2008 included the insertion of a new regulation VI/5 on "Mandatory minimum requirements for the issue of certificates of proficiency for ship security officers". Part A of the STCW Code stipulates the KUP-requirements (Knowledge , Understanding and Proficiency) for certification of SSOs which can be found in Appendix 4.3 – Competency Matrix for Ship Security Officers, so as to determine the need for updating their qualifications.

4.5.20   Some of the practices observed in the appointment and certification of SSOs include:

a   undergoing an approval process based on training course certification and security clearances, particularly if they have access to sensitive security information provided by the Contracting Government (e.g. information on national threats);

b   undertaking training courses by training providers approved by the Administration;

c   having documentary evidence of their appointment and training;

d   being shipping company employees, not contracted resources from an external company (e.g. a security firm or consultant);

e   having an approved documented list of their security and non-security duties. Non-security duties should not interfere with their ability to carry out security duties;

f   being given the opportunity, when newly-appointed, to become familiar with the ship and its SSP plan before assuming the responsibilities; and

g   being the master on ships with small crews. In such cases, the shipping company could consider deploying a trained crew member to assist the master in conducting security activities.

Shipboard personnel with designated security duties

4.5.21   Under the amended STCW Code, shipboard personnel with designated security duties (e.g. deck and gangway watch including contract security guards) are required to hold a certificate of proficiency confirming that they meet the minimum standards of competency listed in Appendix 4.4 – Competency Matrix for Shipboard Personnel with Designated Security Duties.

4.5.22   Given their responsibilities, ship's masters, if they are not also the SSO, should always be considered to have designated security duties.

4.5.23   As a transitional provision, the STCW Code provides that, until January 1, 2014, shipboard personnel with designated security duties who commence their seagoing service prior to January 1, 2012 should be able to demonstrate competence to undertake the tasks, duties and responsibilities listed in Appendix 4.4 – Competency Matrix for Shipboard Personnel with Designated Security Duties, by:

a   having seagoing service as shipboard personnel with designated security duties, for a period of at least six months in total during the preceding three years; or

b   having performed security functions considered to be equivalent to the seagoing service referenced above; or

c   passing an approved test; or

d   successfully completing approved training.

165

4.5.24   Some of the practices observed in the appointment and certification of shipboard personnel with designated security duties include:

a   receiving security-related familiarization training from the SSO (or equally qualified person) in their assigned duties in accordance with the provisions specified in the SSP before being assigned to their duties;

b   having documentary evidence of their training; and

c   being listed in the SSP (by category of personnel).

All shipboard personnel

4.5.25   Under the STCW Code, all shipboard personnel are required to receive approved security-related familiarization training before taking up their duties and be able to:

a   report a security incident including a piracy or armed robbery threat or attack;

b   know the procedures to follow when they recognize a security threat; and

c   take part in security-related emergency and contingency procedures.

4.5.26   Also, before taking up their duties, all shipboard personnel are also required to:

a   receive appropriate approved training or instruction in security awareness as set out in Appendix 4.5 – Competency Matrix on Security Awareness for all Shipboard Personnel; and

b   provide evidence of meeting the minimum standards of competency for security awareness listed in Appendix 4.5 – Competency Matrix on Security Awareness for all Shipboard Personnel. The required evidence may be achieved by demonstrating competence in terms of either the evaluation criteria specified in Appendix 4.5; or through examination or continuous assessment as part of an approved training program.

4.5.27   As a transitional provision, the STCW Code provides that, until January 1, 2014, seafarers who commence their seagoing service prior to January 1, 2012 are required to establish that they meet the requirements listed in Appendix 4.5 – Competency Matrix on Security Awareness for all Shipboard Personnel, by:

a   having approved seagoing service as shipboard personnel, for a period of at least six months in total during the preceding three years; or

b   having performed security functions considered to be equivalent to the seagoing service referenced above; or

c   passing an approved test; or

d   successfully completing approved training.

4.5.28   Experience to date includes examples of shipboard personnel:

a   receiving security awareness training at least once in their career from the SSO or equally qualified person; and

b   having documentary evidence of their security-related training.

Security clearances

4.5.29   Shipping companies can be required to comply with any instructions issued by their flag State regarding the application of any security clearance procedures for their personnel.

4.5.30   Security clearances are the means of verifying that personnel whose duties require access to restricted areas or security sensitive information do not pose a risk to maritime security. The vetting associated with these clearances is more stringent than the pre-employment background checks conducted by shipping companies.

4.5.31   Experience to date includes examples of flag States requiring security clearance for

a   The senior managers of a shipping company; and

b   The CSO and those appointed to undertake any of the duties of the CSO.

4.5.32   A number of Governments require security clearance for all those working in any capacity within port areas including the employees of shipping companies.

4.6   Ship Security Communications

Ship Security Alert Systems

4.6.1   All ships are required to be provided with a Ship Security Alert System (SSAS) as described in paragraphs 2.12.4 to 2.12.15. Its intent is to send a covert signal or message from a ship that will not be obvious to anyone on the ship who is unaware of the alert mechanism.

4.6.2   When activated, the SSAS must:

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

    b   Not send the alert to any other ships;

    c   Not raise any alarm on board the ship; and

    d   Continue the alert until deactivated and/or reset.

4.6.3   The competent authority should be able to receive SSAS alerts on a 24/7 basis.

4.6.4   The SSAS must:

    a   Be capable of being activated from the navigation bridge and in at least one other location;

    b   Conform to performance standards not inferior to those adopted by the IMO; and

    c   Have its activation points designed so as to prevent the inadvertent initiation of an alert.

4.6.5   When a SSAS alert is received by the competent authority, either directly or via a service provider, it should include the following information:

    a   Name of ship;

    b   IMO Ship Identification Number;

    c   Call Sign;

    d   Maritime Mobile Service Identity (which is a series of 9 digits sent over a radio frequency channel to provide a unique identifier used to call ships automatically);

    e   GNSS position of the ship; and

    f   Date and time of the GNSS position.

4.6.6   The requirement for a SSAS may be met by using radio installations that have been approved by the Administration.

4.6.7   The competent authority is responsible for ascertaining whether a security alert is real or false.

4.6.8   The SSP must include:

    a   The identification of the SSAS activation points; and

    b   Procedures to be used including testing, activation, deactivation and resetting to limit false alerts.

    c   Administrations may require this information to be kept in a document separate from the SSP to avoid compromising its confidentiality.

4.6.9   A Master may use an overt alarm (i.e. one such as a VHF broadcast which makes no attempt to deny knowledge of its activation) in addition to a covert alarm as a means of discouraging a security threat from becoming a security incident.

4.6.10   Experience to date of ship operators in establishing SSAS reveal examples of:

    a   Procedures being included in SSPs using a standard template;

    b   The handling of false security alerts being included as a procedure;

    c   Testing being performed at least annually;

    d   When a SSAS is to be tested, all concerned parties being notified by the shipping company so as to avoid any unintended emergency response actions;

e	When a SSAS accidentally transmits in testing, the ship immediately notifying the shipping company or competent authority (if it is not the shipping company), so that all concerned parties can be made aware that the alert is false and that no emergency response action should be taken;

f	A checklist being used when testing; and

g	Providing for an alternative power source.

Automatic Identification Systems

4.6.11	Further to the requirements documented in paragraphs 2.12.16 to 2.12.19, if the master believes that continual operation of AIS might compromise the safety of the ship, or where security incidents are imminent, the AIS may be switched off.

4.6.12	In doing so, Masters should:

a	bear in mind the possibility that attackers are monitoring ship-to-shore communications and using intercepted information to select their targets;

b	be aware that switching off AIS in high-risk areas reduces the ability of the supporting naval vessels to track and trace vessels which may require assistance;

c	exercise caution when transmitting information on cargo or valuables on board by radio in areas where attacks occur;

d	use professional judgement to decide whether the AIS should be switched off to avoid detection when entering areas where piracy is an imminent threat;

e	balance the risk of attack against the need to maintain the safety of navigation;

f	act in accordance with IMO guidance material;

g	be aware that other ships operating in high-risk areas may have taken a decision to switch off their AIS system; and

h	in the event of an attack, ensure to the extent feasible that AIS is turned on again and transmitting to enable security forces to locate the ship.

Pre-Arrival Notification

4.6.13	If a ship intending to enter a port of another Contracting Government is requested to provide the information listed in paragraph 2.12.20, it should be provided by the master or on his behalf by the CSO, SSO or ship's Agent at the port where entry is being sought. It may be submitted in the form of a standard data set such as the one shown in Appendix 4.6 – Standard Data Set of Security-related Pre-Arrival Information. If submitted electronically, it may not be possible for a signature to be provided.

4.6.14	The master may decline to provide such information but failure to do so may result in denial of entry into port.

4.6.15	The ship is required to keep records of the information provided for the last 10 calls at port facilities.

Long Range Identification and Tracking systems

4.6.16	Long Range Identification and Tracking (LRIT) system requirements are described in paragraphs 2.12.25 to 2.12.37.

4.6.17	The ship operator's obligation is to comply with these requirements by providing on board equipment for transmitting the identity of the ship, its position and the date and time of the position to the Data Centre (DC) nominated by the ship's Administration.

4.6.18	In exceptional circumstances and for the shortest duration possible, the LRIT system can be switched off if its operation is considered by the master to compromise the safety or security of the ship. In such instances, the master is required to inform the Administration without undue delay and record the occurrence with the reason for the decision and duration of non-transmittal.

4.7 Ship Security Assessments

Introduction

4.7.1   A Ship Security Assessment (SSA) must be undertaken for each ship as a prelude to the preparation of a SSP (refer to paragraphs 2.9.12 to 2.9.14).

4.7.2   A SSA may be considered to be a risk analysis of all aspects of a ship's operations in order to determine which parts of it are more vulnerable. It is an essential and integral part of developing or updating the SSP.

4.7.3   CSOs are responsible for ensuring that SSAs are carried out for each ship in their company's fleet by persons with appropriate skills to evaluate the security of a ship.

4.7.4   RSOs may carry out SSAs provided that they are not subsequently involved in the review and approval of the associated SSP (refer to paragraphs 4.2.6 to 4.2.8).

Conducting and Documenting SSAs

4.7.5   The SSA is required to include the following elements:

    a   An on-scene security survey;

    b   Identification of existing security measures, procedures and operations;

    c   Identification and evaluation of important shipboard operations;

    d   Identification of possible threats to important shipboard operations and the likelihood of their occurrence;

    e   Identification of weaknesses including human factors in the infrastructure, policies and procedures.

4.7.6   As with PFSAs, Administrations could consider requiring SSAs to establish and prioritize countermeasures.

4.7.7   The SSA for each ship in the company's fleet is required to be documented, reviewed, accepted and retained by the shipping company.

Preparing SSA Reports

4.7.8   A report must be prepared on completion of the SSA. It provides the means by which a SSA is accepted by the shipping company and is required to:

    a   Summarize how the assessment was conducted;

    b   Describe each vulnerability found during the assessment;

    c   Describe the countermeasures that could address each vulnerability;

    d   Be protected from unauthorized access or disclosure.

4.7.9   If used, a completed template could be attached to the SSA report as an annex.

4.7.10   If the SSA has not been carried out by the shipping company, the SSA report should be reviewed and accepted by the CSO.

4.7.11   Experience to date includes examples of CSOs:

    a   providing a numbered copy of an approved SSA Report to a list of individuals within the company;

    b   before commencing a SSA, seeking out available information on threat assessments at ports which will be visited by the ship; studying previous reports on similar security needs; and discussing how the SSA is to be conducted with appropriate persons on board ship and in the port facilities and ports to be visited;

    c   following the specific guidance offered by national authorities and seeking clarification when appropriate; and

      d   in conjunction with the SSO, when developing countermeasures, considering their effect in terms of:
- comfort and convenience;
- personal privacy; and
- the performance of duties by shipboard personnel who may have to remain on board for long periods.

Updating SSAs

4.7.12   A SSA should be reviewed and updated as appropriate when there has been:

      a   a significant security incident involving the ship;

      b   a change in the ship's trading pattern; or

      c   change of the owner or operator of the ship.

4.7.13   These changes could include changes to sea routes, particularly in instances where the change may result in new threat scenarios and increased probability of a security incident.

4.8   Ship Security Plans

Introduction

4.8.1   Each ship is required to carry on board a ship security plan (SSP) approved by the Administration. It must make provision for the three Security levels (refer to sub-section 4.3). The close inter-relationship between SSAs and SSPs is shown by the example of a SSA/SSP approval process illustrated in Appendix 4.6 – Standard Data Set of Security-related Pre-Arrival Information.

4.8.2   RSOs may:

      a   Prepare SSPs on behalf of CSOs (who are responsible for ensuring that the SSPs are prepared and submitted for approval);

      b   Review and approve SSPs and their amendments on behalf of an Administration provided that they were not involved in the preparation of the SSP under review or its related SSA.

4.8.3   When a SSP or its amendment is submitted for approval, it must be accompanied by the SSA on which the plan or amendment was based.

4.8.4   CSOs and their SSOs should retain records of any amendments made to an approved ship security plan.

Preparing and Maintaining SSPs

4.8.5   SSPs should provide details of:

      a   Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports from being taken on board;

      b   Restricted areas and measures for the prevention of unauthorized access to them;

      c   Measures and equipment for the prevention of unauthorized access to the ship including boarding of a ship when in port or at sea;

      d   Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

      e   The minimum operational and physical security measures the ship shall take at all times, when operating at Security level 1;

      f   The additional or intensified security measures the ship itself can take when moving to Security level 2;

      g   Procedures for promptly responding to any security instructions Governments may give at Security level 3;

      h   Procedures for evacuation in case of security threats or breaches of security;

i   Security-related duties of shipboard personnel assigned security responsibilities and other shipboard personnel;

j   Procedures for auditing the security activities;

k   Procedures for training, drills and exercises associated with the plan;

l   Procedures for interfacing with port facility security activities;

m   Procedures for the periodic review of the plan and updating;

n   Procedures for reporting security incidents;

o   The SSO and CSO, including 24-hour contact details;

p   Procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board;

q   Frequency of testing or calibrating any security equipment provided on board; and

r   Procedures, instructions and guidance on SSAS usage, including the testing, activation, deactivation, resetting and limitation of false alerts.

4.8.6   In addition, SSPs should detail:

a   The organizational structure of security for the ship;

b   The ship's relationship with the Company, port facilities, other ships and relevant authorities with security responsibility;

c   The communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;

d   The basic security measures for security level 1, both operational and physical, that will always be in place;

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

f   provision for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

g   Reporting procedures to the appropriate Contacting Government's contact points.

h

4.8.7   Due to conflict of interest considerations, personnel conducting internal audits of the security measures specified in SSPs or evaluating their implementation are required to be independent of the measures being audited unless this is impracticable due to the size and nature of the shipping company or its fleet.

4.8.8   SSPs are required to be protected from unauthorized access or disclosure.

4.8.9   The relevant provisions of the SSP placed on board must be in the working language of the ship's personnel or languages understood by them.

4.8.10   If SSPs are kept in electronic format, procedures must be put in place to prevent their unauthorized deletion, destruction or amendment.

4.8.11   Experience to date indicates that several Administrations have developed model ship security plans, pre-submission checklists and related guidance material. Those referenced on internet sites are listed in Appendix 4.8 – Examples of Internet Sources of Guidance Material on Preparing and Validating Ship Security Plans, along with a summary of their contents.

Planning and conducting ship security drills and exercises

4.8.12   The regular conduct of ship security drills and exercises is an important aspect of ensuring that ships comply with the requirements of the Maritime Security Measures.

4.8.13   Drills may be defined as supervised activities used to test a single measure or procedure in the SSP. Exercises are more complex activities which test several measures and procedures at the same time.

4.8.14   To ensure the effective implementation of the measures and procedures specified in SSPs, drills should be conducted at least once every three months. These are usually organized by SSOs who are responsible for ensuring that all shipboard personnel have received adequate training.   In addition, in cases

where more than 25% of the ship's personnel has been changed at any one time with personnel that have not previously participated in any drill on that ship within the last three months, a drill should be conducted within one week of the change.

4.8.15   As a minimum, SSOs should organize drills to cover such scenarios as:

      a   Identification and search of unauthorized visitors onboard the ship;

      b   Recognition of materials that may pose a security threat;

      c   Methods to deter attackers from approaching the ship;

      d   Recognition of restricted areas;

      e   Mustering for evacuation.

4.8.16   Further guidance on undertaking drills and exercises is available from http://www.uscg.mil.hq/cg5/nvic/pdf/NVIC_04_03_CHANGE_3.pdf

4.8.17   To ensure the effective implementation and coordination of SSPs, CSOs are required to participate in exercises at a recommended minimum interval of once each calendar year with no more than 18 months between the exercises.

4.8.18   These exercises, which could test communications, co-ordination, resource availability, and response, may be:

      a   full-scale or live;

      b   tabletop simulation or seminar; or

      c   combined with other exercises organized by government agencies to test search and rescue or emergency response capabilities.

4.8.19   Exercises may cover such on-board emergencies as searches for bombs, weapons and unauthorized personnel as well as responses to damage or destruction of ship infrastructure. They do not have to involve each ship within a fleet. If an exercise is carried out on board and/or involves one or more of a shipping company's ships then, as a minimum, the exercise details and lessons learnt can be circulated throughout the fleet by means of seminars on board each ship; also, any measures that are identified can be implemented on each ship.

4.8.20   Drills and exercises take up organizational time and resources, and must therefore be conducted in as efficient and effective a manner as possible. Recognizing the need to assist port facility operators in the Asia-Pacific Region, APEC's Transportation Working Group developed a set of guidelines in the form of a manual (refer to Appendix 3.7). Although its focus is on port operations, the manual provides a systematic and comprehensive approach to the planning, preparation for, conduct, debrief and reporting of maritime security drills and exercises. Thus, it could provide a useful reference for planning and conducting drills and exercises on board ships.

4.8.21   The conduct of drills and exercises may require an approved SSP to be amended; for a major amendment, the SSP must be submitted to the Administration or authorised RSO for re-approval.

Access to ships by government officials, emergency response services and pilots

4.8.22   Government officials entitled as part of their duties to board ships should carry appropriate identification documents issued by the Government. Identification documents should include a photograph of the holder of the document. They should also include the name of the holder or have a unique identification number. If the identity document is in a language other than English, French or Spanish a translation into one of those languages should be provided.

4.8.23   Government officials should present their identification document when requested to do so when boarding a ship.

4.8.24   Ship security personnel should be able to verify the authenticity of identity documents issued to Government officials and Governments should establish procedures, and provide contact details, to facilitate such validation.

4.8.25   Emergency response services and pilots should also carry appropriate identification documents and present them when boarding a ship. The authenticity of such identification documents should be capable of being verified.

4.8.26   Only the person in charge of an emergency response team need present an identification document when boarding a ship and should inform the relevant security personnel of the number of emergency response personnel entering or boarding.

4.8.27   Government officials, emergency response personnel and pilots should not be required to surrender their identity documents when boarding a ship. The issuance of visitor identification documents by a ship may not be appropriate when Government officials, emergency response personnel or pilots have produced an identity document which can be verified.

4.8.28   Government officials should not be subject to search by ship security personnel. Any search requirement in a SSP could be waived for emergency response personnel responding to an emergency or for a pilot boarding a ship once their identity has been verified.

4.8.29   SSOs should be able to secure the assistance of PFSOs to verify the identification of Government officials, emergency response personnel or pilots intending to board a ship.

Shore leave and access to shore-based facilities by seafarers

4.8.30   The obligations of Governments and their national authorities related to shore leave and access to shore-based facilities are addressed in paragraphs 2.17.5 to 2.17.8, while those of port and port facility operators are addressed in paragraphs 3.8.13 to 3.8.19.

4.8.31   Normally, the SSO contacts the PFSO before arrival at the port facility in order to coordinate shore access and on-board visits arrangements. These arrangements must strike a balance between the need for port and port facility security, and the needs of the ship and its crew.

4.8.32   Procedures to facilitate shore access by, or shore leave for, seafarers should be transparent, easy to follow and should not require involvement by the seafarers. The procedures should provide a system whereby seamen, pilots, welfare and labour organizations can board and depart vessels in a timely manner. These procedures should not impose undue costs upon the individual requiring passage to and from the vessel. Barriers such as excessive fees or restrictive hours of operation should not be imposed.

4.8.33   In instances where shore leave is denied to crew members, the SSO should immediately refer the matter to the CSO to raise with appropriate authorities.

Reporting Security Incidents

4.8.34   SSPs are required to document the procedures for reporting security incidents and threats to Administrations and other government organizations (refer to paragraph 2.9.37).

4.8.35   Security incidents generally can fall into two categories:
   a   Those considered to be sufficiently serious that they should be reported to relevant authorities by the CSO including:
   - unauthorized access to restricted areas within the ship for suspected threat-related reasons;
   - unauthorized carriage or discovery of stowaways, weapons or explosives;
   - incidents of which the media are aware;
   - bomb warnings;
   - attempted or successful boardings; and
   - damage to the ship caused by explosive devices or arson.
   b   Those of a less serious nature but require reporting to, and investigation, by the SSO can include:
   - unauthorized access to the ship caused by breaches of access control points or inappropriate uses of passes;
   - damage to equipment through sabotage or vandalism;
   - unauthorized disclosure of a SSP;
   - suspicious behaviour near the ship when at a port facility;
   - suspicious packages near the ship when at a port facility; and
   - unsecured access points to the ship.

173

4.8.36   If a security threat or incident develops which requires initiation of the security procedures and measures applying at a higher Security level than the Security level set for the port facility, the initiation of the appropriate response to the emerging threat by a port facility or ship should not, and cannot, await change of the Security level by the relevant Government or its Administration. The response to the security threat or incident as it develops should be taken in accordance with the SSP. The ship should report the threat or incident—and the action taken—to the Government, designated authority or administration at the earliest practicable opportunity.

4.8.37   Experience to date indicates that some Administrations have:

a   Specified the types of security incidents that must be immediately reported them, as indicated below:

Type of security incident
Attack
Bomb warnings
Hijack
Armed robbery or piracy against a ship
Discovery of firearms
Discovery of other weapons
Discovery of explosives
Unauthorized access to a restricted area
Unauthorized access to the port facility
Media awareness

b   With respect to bomb warnings, developed a checklist as a useful aid for anyone receiving a warning (which can be received in various ways with a telephone call to a shipping agent, shipping company or individual ship being the most common). A sample checklist may be accessed at: www.cpni.gov.uk/Docs/Bomb_threat_checklist.pdf

c   Designed standard forms for security incidents that must be reported to them and making them available on their internet sites. Examples of such forms may be downloaded from the following internet sites:

-    www.infrastructure.gov.au/transport/security/maritime/MSIR_online_form.aspx.
-    www.mpa.gov.sg/sites/circulars.../shipping.../security_incident_form.pdf
-    www.gibmaritime.com
-    www.mcw.gov.cy/mcw/dms/dms.nsf/All/78C174E7BB90EA95C22575190042D23A?OpenDocument   .

d   Although these forms have been designed to fulfil incident reporting requirements prescribed in national legislation, they could be adapted by ship operators to their particular reporting requirements. In such cases, the form's practical usefulness could be enhanced by:

-    Ensuring that its format is straightforward;
-    Allowing the SSO to report the remedial action taken;
-    Ensuring that any associated reporting procedures are straightforward;
-    Establishing the situations when it is to be forwarded to the CSO; and
-    Locating copies where they can be visible to, and easily accessed by, shipboard personnel.

e   specified the manner in which the reports should be made and the procedures for doing so including the time period by which an incident must be reported and the recipients of such reports (e.g.. local law enforcement agencies when a ship is in a port facility or an adjacent coastal State).

Maintaining On-board Records

4.8.38   Administrations should specify the security records that a ship is required to keep and be available for inspection including the period for which they should be kept (sub-section **Error! Reference source not found.**). The records must cover:

    a   DOS agreed with port facilities and other ships;

    b   security threats or incidents;

    c   breaches of security;

    d   changes in Security level;

    e   communications relating to the direct security of the ship such as specific threats to the ship or to port facilities where the ship is, or has been;

    f   ship security training undertaken by the ship's personnel;

    g   security drills and exercises;

    h   maintenance of security equipment;

    i   internal audits and reviews;

    j   reviews of SSAs and SSPs; and

    k   any amendments to an approved SSP.

4.8.39   Records are required to be:

    a   kept in the working language(s) of the ship;

    b   protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment if kept in an electronic format;

    c   protected from unauthorized access or disclosure;

    d   be available to duly authorized officers of Contracting Governments to verify that the provisions of SSPs are being implemented, and

    e   kept on board for the period specified by the Administration.

Conducting Self-Assessments

4.8.40   Checklists can provide a useful way to assess and report progress in implementing SSPs and, by extension, the Maritime Security Measures.

4.8.41   Appendix 4.9 – Implementation Checklist for Ship Security Personnel, contains a checklist for ship security personnel that allows them to assess progress in implementing the Maritime Security Measures. Except for minor modifications to its format and guidance material, it is identical to the Voluntary Self-Assessment Tool for Ship Security that was approved by the IMO's Maritime Safety Committee in May 2006 and received widespread distribution.

4.8.42   Appendix 4.10 – Implementation Checklist for Shipping Companies & their CSOs, contains a checklist for shipping companies and their CSOs to assess progress in implementing the Maritime Security Measures. It was issued by the IMO in December 2006.

4.8.43   Experience to date reveals that:

    a   several Administrations have encouraged the annual use of these checklists as a good management practice; and

    b   CSOs and SSOs have modified its content and format to meet their specific assessment requirements (e.g. to identify when procedures were last reviewed or measures tested, or to establish a link between any identified gaps and work plan priorities).

Reviewing and amending an approved SSP

4.8.44   Administrations should notify CSOs of amendments to an approved SSP that must be approved before they can be implemented.   This notification can be provided on approval of the initial SSP or a subsequent amendment.

4.8.45   Similarly, Administrations should notify CSOs of the amendments to an approved SSP that do not require their prior approval.

4.8.46   Unless the Administration has allow specified amendments to be made without their prior approval, proposed amendments to an approved SSP may not be implemented until authorized by the Administration.

4.8.47   The preparation of all amendments to an approved SSP is ultimately the responsibility of the CSO.

4.8.48   If the Administration allows a CSO or SSO to amend a SSP without its prior approval, the adopted amendments must be communicated to the Administration at the earliest opportunity.

4.8.49   Experience to date indicates that:
   a   SSPs are being reviewed annually and more frequently in response to incidents such:
      -    changes in ship operations, ownership and structure;
      -    after an unsuccessful drill or exercise;
      -    after a security incident or threat involving the ship;
      -    completion of a review of the SSA;
      -    when an internal audit or inspection by the Administration has identified failings in the ship's security organization and operations calling into question the continuing relevance of the approved SSP.
   b   Amendment of an approved SSP also involves a review of the ship's SSA.
   c   Administrations have required the following types of proposed changes to be submitted for their approval prior to their implementation:
      -    procedures for acknowledging changes in security levels;
      -    measures or procedures at Security levels 2 and 3;
      -    procedures for controlling access to the ships;
      -    procedures for reporting incidents;
      -    frequency of testing security equipment;
      -    procedures for maintaining security equipment;
      -    procedures for maintaining document confidentiality;
      -    frequency of conducting drills and exercises;
      -    SSAS procedures;
      -    the CSO's identity and contact details
   d   Some Administrations have shown flexibility in allowing minor amendments to an approved SSP without their prior approval. This can often relate to changes that can occur frequently e.g. changing the SSO.
   e   It has proved convenient to format SSPs so as to facilitate the submission of amendments in the form of single pages rather than the whole document.

4.9   The International Ship Security Certificate

4.9.1   Ships falling under the Maritime Security Measures have to carry either the International Ship Security Certificate (ISSC) or, in limited circumstances, the Interim ISSC, both of which are issued by their Administration. Details of their issuance, required verifications, duration of validity, loss of validity and remedial actions are provided in sub-section 2.10.

4.9.2   Shipping companies are required to:
   a   Ensure that verification of compliance with the Maritime Security Measures takes place:
      -    before their ships are put into service and the ISSC issued (initial verification);
      -    at least once between the second and third anniversary of the issuance of the ISSC if the validity period is for five years (intermediate verification); and
      -    before the ISSC is renewed (renewal verification).
   b   Notify the ship's Administration immediately when there is a failure of a ship's security equipment or system or suspension of a security measures which compromises the ship's ability to operate at Security levels 1 to 3. The notification should be accompanied by any proposed remedial actions; and

c   Notify the ship's Administration when the above circumstances do not compromise the ship's ability to operate at security levels 1 to 3. In such cases, the notification should be accompanied by an action plan specifying the alternative security measure being applied until the failure or suspension is rectified together with the timing of any repair or replacement.

4.9.3   Experience to date indicates that Administrations:

a   Provide guidance to their CSOs reminding them of the cumulative effect that individual failures or suspensions of measures could have on the ability of their ships to operate at Security levels 1 to 3;

b   Apply widely diverging interpretations of when a SOLAS ship is out of service or laid up; and of the circumstances and passage of time that could lead to consideration of suspension or withdrawal of the ship's ISSC.   The Maritime Security Measures are silent on the specific issues.

4.10   Control and Compliance Measures

4.10.1   Governments can apply specific control and compliance measures to foreign-flagged SOLAS ships using, or intending to use, their ports when assessing their compliance with the Maritime Security Measures. Elements of these control and compliance measures are unique including the authority to:

a   require ships to provide security related information prior to entering port;

b   inspect ships intending to enter into port when there are clear grounds for doing once the ship is within the territorial sea. The Master has a right to refuse such an inspection and withdraw his intention to enter that port, and

c   refuse to allow a ship to enter port; and

d   expel a ship from port.

4.10.2   Details of the responsibilities, procedures and limitations of Administrations in exercising this authority, and the measures that may be applied are provided in sub-section **Error! Reference source not found.**.

4.10.3   During interactions with duly authorized officers, ships' masters and their SSOs should be able to:

a   communicate in English; and

b   verify the identity of duly authorized officers intending to board their ship.

4.10.4   If requested to do so, a ship has to provide security-related information prior to entering into a port. The IMO has developed a standard data set of the security-related information that a ship might be expected to provide (refer to Appendix 4.6 – Standard Data Set of Security-related Pre-Arrival Information).   The standard data set does not preclude a Government from requesting further security-related information on a regular basis or in specified circumstances. When Governments require additional information, the shipping industry should be appropriately advised.

4.10.5   If a ship has been advised of the intention to take control measures under the Maritime Security Measures, it can:

a   decide to withdraw its intention to enter the port; or

b   discuss ways of rectifying its non-compliance with the duly authorized officer.

4.10.6   If a ship is unduly delayed, the Maritime Security Measures provide for compensation to be claimed for loss or damage.

4.10.7   The Maritime Security Measures require documents to be carried on board ship some of which can be inspected by duly authorized officers undertaking control and compliance measures when a ship is in, or intending to enter port. The documents which are required to be available for inspection include:

a   The original of the valid ISSC or Interim ISSC;

b   The current CSR and any amendment form;

c   The certificates of proficiency for the SSO and shipboard personnel with designated security duties;

d   Parts of the SSP subject to authorization being received from the ship's Administration; and

e   All DOS that the ship has agreed during the period covered by the ship's last 10 ports of call.

4.10.8   Information on the current CSR and any amendment form should include:

a   the Administration, Government or RSO that issued the valid ISSC or Interim ISSC; or

b   if different from above, the body that carried out the verification on which the certificate was issued.

4.10.9   Experience to date indicate that security- related deficiencies represent around 3-5% of the total number of deficiencies found on SOLAS ships, with the vast majority being safety-related.

4.11   Guidelines for Non-SOLAS vessels

Introduction

4.11.1   As mentioned in paragraph 4.2.2, there is no requirement under the Maritime Security Measures for Contracting Governments to extend their application to non-SOLAS vessels. However, it has been generally recognized that voluntary application of security practices and principles contained in these measures represents a desirable goal, one that helps to strengthen the overall maritime security framework.

4.11.2   The following sections provide general guidance that are relevant for all types of non-SOLAS vessels. Appendix 4.11 – General information on security practices for all non-SOLAS vessel operators, lists security practices for all non-SOLAS vessels as well as specific practices that are relevant to the following four types of non-SOLAS vessels:

a   Commercial non-passenger and special purpose vessels

b   Passenger vessels

c   Fishing vessels

d   Pleasure craft

General Guidance

4.11.3   The implementation of appropriate security measures should be governed by the results of a risk assessment.

4.11.4   Non-SOLAS vessel operators should consider maintaining an appropriate level of security awareness and incident response capability on-board their vessels by:

a   providing all on-board personnel with information on how to reach appropriate officials and authorities in the event of security problems or if suspicious activity is observed.
This information should include contact information for the officials responsible for emergency response, the national response centre(s) (if appropriate) and any authorities that may need to be notified.

b   implementing security initiatives developed by national authorities with respect to education, information sharing, coordination and outreach programs.

c   promoting links with Administrations' maritime security services.

d   establishing a workplace culture that recognizes the need to balance security requirements with both the safe and efficient operation of the vessel and the rights and welfare of seafarers;

e   developing security training policies and procedures to ensure that all personnel (including passengers where appropriate) are familiar with basic security measures that are applicable;

f   recommending basic security familiarization training for crew members enabling them to have the capability to respond to security threats. In higher-risk environments, this training should cover the competencies required to implement any security measures that are in place.

4.11.5   Operators may also wish to adopt hiring practices such as background checks. However, when such practices are in place, it is important for there to be:

a   provisions allowing seafarers and other workers to appeal adverse employment determinations based on disputed background information; and

b   adequate protections for workers' rights to privacy.

4.11.6   Non-SOLAS vessels on international voyages may be required to declare arrival and departure information for purposes of obtaining a port clearance from the relevant authorities. This declaration may be required within a specified period as determined by local authorities following arrival and/or prior to departure. The information to be submitted may include the particulars of vessel, date/time of arrival, position in port, particulars of Master/owner/shipping line/agent, purpose of call, amount of cargo on board, passenger and crew list, and emergency contact numbers.

4.11.7   Operators of non-SOLAS vessels on international voyages may be encouraged by their Administration to fit automated tracking equipment on their vessels. The benefits of such a system could include enhanced safety and security; more rapid emergency response to maritime accidents and casualties; better and more effective SAR capabilities; and better control of smuggling, human-trafficking attempts, and illegal, unregulated or unreported fishing.

4.11.8   Non-SOLAS vessel operators should be aware of the key aspects of the Maritime Security Measures relevant to their vessels, including:

a   Communication of changes in security levels and implications for their operations;

b   Requirements for interacting with ships and port facilities falling under the Maritime Security Measures.

4.11.9   If the non-SOLAS vessel operator is required to complete a Declaration of Security with a PFSO or SSO, the following procedures apply:

a   the SSO or PFSO should contact the non-SOLAS vessel well in advance of the non-SOLAS vessel's interaction with the ship or port facility, giving the master of the non-SOLAS vessel reasonable time to prepare for those security measures that might be required;

b   the SSO or PFSO should detail the security measures with which the non-SOLAS vessel is being asked to comply using the appropriate DOS form;

c   the DOS should be completed and signed by both parties.

4.11.10   It is important that all operators of non-SOLAS vessels are aware of the need to stay a reasonable distance from SOLAS ships when using shared waterways. The appropriate distance will vary due to navigational safety considerations. Non-SOLAS vessels should take care not to undertake any manoeuvres close to the vessel which may give the crew of the SOLAS ship cause for concern. Non-SOLAS vessels are encouraged to clearly indicate their intentions to the crew of SOLAS ships by radiotelephone or other means.

4.11.11   Some Administrations have issued guidance material for non-SOLAS vessels which are fitted with ship security alert systems. Vessel operators should check with their national authority to determine if guidelines have been issued.

Appendix 4.1 – Sample of a Declaration of Security Form for a Ship-to-Ship Interface

Name of Ship A: _____

Port of Registry: _____

IMO Number: _____

Name of Ship B _____

Port of Registry: _____

IMO Number: _____

This Declaration of Security is valid from …………… until ……………, for the following activities
……………………………………………………
 (list the activities with relevant details)

under the following Security levels

Security level(s) for Ship A: _____

Security level(s) for Ship B: _____

Both ships agree to the following security measures and responsibilities to ensure compliance with the relevant requirements of their national maritime security legislation (or, if not enacted, of Chapter 5 in Part A of the ISPS Code).

Activity	The initials of each SSO or Master in these columns indicates that the activity will be done, in accordance with their approved ship security plan, by Ship A and/or Ship B	
	Ship A:	Ship B:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorised personnel have access		
Controlling access to ship A		
Controlling access to ship B		
Monitoring of ship A, including areas surrounding the ship		
Monitoring of ship B, including areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ships		

The signatories to this agreement certify that security measures and arrangements for both ships during the specified activities meet the relevant provisions of their national maritime security legislation (or, if not enacted,

of Chapter 5 in Part A of the ISPS Code) and will be implemented in accordance with the provisions already stipulated in their approved ship security plan(s) or with specific arrangements agreed to (as set out in the attached annex) .

Dated at …………………………………… on the ……………………………………

Signed for and on behalf of	
Ship A:	Ship B:
(Signature of Master or Ship Security Officer)	(Signature of Master or Ship Security Officer)
Name and title of person who signed	
Name:	Name:
Title:	Title

Contact Details	
(to be completed as appropriate)	
(indicate the telephone numbers, radio channels or frequencies to be used)	
for Ship A:	for Ship B:
Master	Master
Ship Security Officer	Ship Security Officer
Company	Company
……………………………………………………	
Company Security Officer	Company Security Officer
…………………………………………………..	

Source: MSC/Circ.1154, May 2005

Competence • Knowledge Requirement	Methods for demonstrating competence • Evaluation Criteria
Develop, maintain and supervise the implementation of a SSP • International maritime security policy and responsibilities of Governments, companies and designated persons. • Purpose for and the elements that make up a SSP. • Procedures to be employed in developing, maintaining, and supervising the implementation of, and the submission for approval of a SSP. • Procedures for the initial and subsequent verification of the ship's compliance. • Maritime security levels and the consequential security measures and procedures aboard ship and in the port facility environment. • Requirements and procedures involved with arranging for internal audits and review of security activities specified in a SSP. • Requirements and procedures for acting upon reports by the SSO to the CSO concerning any deficiencies or non-conformities identified during internal audits, periodic reviews, and security inspections. • Methods and procedures used to modify the SSP. • Security related contingency plans and the procedures for responding to security threats or breaches of security including provisions for maintaining critical operations of the ship/port interface. • Maritime security terms and definitions used in the Maritime Security Measures.	**Assessment of evidence obtained from approved training or examination** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Legislative requirements relating to security are correctly identified. • Procedures achieve a state of readiness to respond to changes in security levels. • Communications within the CSO's area of responsibility are clear and understood.
Ensuring security equipment and systems, if any, are properly operated • Various types of security equipment and systems and their limitations.	**Assessment of evidence obtained from approved training or examination and practical demonstration of ability to conduct physical searches and non intrusive inspections** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Procedures achieve a state of readiness to respond to changes in security levels. • Communications within the CSO's area of responsibility are clear and understood.

Assess security risk, threat, and vulnerability	**Assessment of evidence obtained from approved training or examination and practical demonstration of ability to conduct physical searches and non-intrusive inspections**
• Risk assessment, assessment tools, and procedures for conducting security assessments. • Security assessment documentation including the DOS. • Techniques used to circumvent security measures. • Enabling recognition, on a non-discriminatory basis, of persons posing potential security risks. • Enabling recognition of weapons, dangerous substances, and devices and awareness of the damage they can cause. • Crowd management and control techniques, where appropriate. • Handling sensitive security related information and security related communications. • Methods for implementing and co-ordinating searches. • Methods for physical searches and non-intrusive inspections.	• Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Procedures achieve a state of readiness to respond to changes in the maritime security levels. • Communications within the CSO's area of responsibility are clear and understood.
Ensure appropriate security measures are implemented and maintained	**Assessment of evidence obtained from approved training or examination**
• Requirements and methods for designating and monitoring restricted areas. • Methods for controlling access to the ship and to restricted areas on board ship. • Methods for effective monitoring of deck areas and areas surrounding the ship. • Security aspects relating to the handling of cargo and ship's stores with other shipboard personnel and relevant PFSOs. • Methods for controlling the embarkation, disembarkation and access while on board of persons and their effects.	• Procedures and actions are in accordance with the principles established by the Maritime Security Measures • Procedures achieve a state of readiness to respond to changes in the maritime security levels. • Communications within the CSO's area of responsibility are clear and understood.
Encourage security awareness and vigilance	**Assessment of evidence obtained from approved training or examination.**
• Training, drill and exercise requirements under relevant conventions and codes. • Methods for enhancing security awareness and vigilance on board. • Methods for assessing the effectiveness of drills and exercises. • Instructional techniques for security training and education.	• Procedures and actions are in accordance with the principles established by the SOLAS Security Measures. • Communications within the CSO's area of responsibility are clear and understood.

Appendix 4.3 – Competency Matrix for Ship Security Officers

Source: Section A-V1/5 of the STCW Code, as amended, August 2010

Competence • Knowledge Requirement	Methods for demonstrating competence • Evaluation Criteria
Maintain and supervise the implementation of a Ship Security Plan • International maritime security policy and responsibilities of Governments, companies and designated persons including elements that may relate to piracy and armed robbery. • Purpose for and the elements that make up a SSP, related procedures and maintenance of records including those that may relate to piracy and armed robbery. • Procedures to be employed in implementing a SSP and reporting of security incidents. • Maritime security levels and the consequential security measures and procedures aboard ship and in the port facility environment. • Requirements and procedures for conducting internal audits, on-scene surveys, control and monitoring of security activities specified in a SSP. • Requirements and procedures for reporting to the CSO any deficiencies and non-conformities identified during internal audits, periodic reviews and security inspections. • Methods and procedures used to modify the SSP. • Security related contingency plans and the procedures for responding to security threats or breaches of security including provisions for maintaining critical operations of the ship/port interface and elements that may relate to piracy and armed robbery. • Maritime security terms and definitions including elements that may relate to piracy and armed robbery.	**Assessment of evidence obtained from approved training or examination** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Legislative requirements relating to security are correctly identified. • Procedures achieve a state of readiness to respond to changes in Security levels. • Communications within the SSO's area of responsibility are clear and understood.
Assess security risk, threat, and vulnerability • Risk assessment and assessment tools. • Security assessment documentation including the DOS. • Techniques used to circumvent security measures including those used by pirates and armed robbers. • Enabling recognition, on a non-discriminatory basis, of persons posing potential security risks. • Enabling recognition of weapons, dangerous substances, and devices and awareness of the damage they can cause. • Crowd management and control techniques, where appropriate. • Handling sensitive security-related information and security-related communications. • Implementing and co-ordinating searches. • Methods for physical searches and non-intrusive inspections.	**Assessment of evidence obtained from approved training or approved experience and examination including practical demonstration of competence to conduct physical searches and non-intrusive inspections** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Procedures achieve a state of readiness to respond to changes in Security levels. • Communications within the SSO's area of responsibility are clear and understood.

Undertake regular inspections of the ship to ensure that appropriate security measures are implemented and maintained	Assessment of evidence obtained from approved training or examination
• Requirements for designating and monitoring restricted areas. • Controlling access to the ship and to restricted areas on board ship. • Methods for effective monitoring of deck areas and areas surrounding the ship. • Security aspects relating to the handling of cargo and ship's stores with other shipboard personnel and relevant PFSOs. • Methods for controlling the embarkation, disembarkation and access while on board of persons and their effects.	• Procedures and actions are in accordance with the principles established by the Maritime Security Measures • Procedures achieve a state of readiness to respond to changes in the Security levels. • Communications within the SSO's area of responsibility are clear and understood.
Ensure that security equipment and systems, if any, are properly operated, tested and calibrated	**Assessment of evidence obtained from approved training or examination**
• Various types of security equipment and systems and their limitations, including those that could be used in case of attacks by pirates and armed robbers. • Procedures, instructions and guidance on the use of SSAS. • Methods for testing, calibrating, and maintaining security systems and equipment, particularly whilst at sea.	• Procedures and actions are in accordance with the principles established by the Maritime Security Measures • Procedures achieve a state of readiness to respond to changes in the Security levels. • Communications within the SSO's area of responsibility are clear and understood.
Encourage security awareness and vigilance	**Assessment of evidence obtained from approved training or examination.**
• Training, drill and exercise requirements under relevant conventions and codes and IMO circulars including those relevant to anti-piracy and anti-armed robbery. • Methods for enhancing security awareness and vigilance on board. • Methods for assessing the effectiveness of drills and exercises.	• Procedures and actions are in accordance with the principles established by the SOLAS Security Measures. • Communications within the CSO's area of responsibility are clear and understood.

Appendix 4.4 – Competency Matrix for Shipboard Personnel with Designated Security Duties

Source: Section A-VI/6 of the STCW Code, as amended, August 2010

Competence • Knowledge Requirement	Methods for demonstrating competence • Evaluation Criteria
Maintain the conditions set out in a Ship Security Plan • Maritime security terms and definitions including elements that may relate to piracy and armed robbery. • International maritime security policy and responsibilities of Governments, companies and persons including elements that may relate to piracy and armed robbery. • Maritime security levels and their impact on security measures and procedures aboard ship and in the port facilities. • Security reporting procedures. • Procedures for drills and exercises under relevant conventions, codes and IMO circulars including those that may relate to piracy and armed robbery. • Procedures for conducting inspections and surveys and for the control and monitoring of security activities specified in a SSP. • Security-related contingency plans and the procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship/port interface and those that may relate to piracy and armed robbery.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures. • Legislative requirements relating to security are correctly identified. • Communications within the area of responsibility are clear and understood.
Recognition of security risks and threats • Security documentation including the DO S. • Techniques used to circumvent security measures including those used by pirates and armed robbers. • Enabling recognition of potential security threats. • Enabling recognition of weapons, dangerous substances, and devices and awareness of the damage they can cause. • Crowd management and control techniques, where appropriate. • Handling security-related information and security-related communications. • Methods for physical searches and non-intrusive inspections.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Procedures and actions are in accordance with the principles established by the Maritime Security Measures.
Undertake regular security inspections of the ship • Techniques for monitoring restricted areas. • Controlling access to the ship and to restricted areas on board ship. • Methods for effective monitoring of deck areas and areas surrounding the ship. • Inspection methods relating to the cargo and ship's stores. • Methods for controlling the embarkation, disembarkation and access while on board of persons and their effects.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** Procedures and actions are in accordance with the principles established by the Maritime Security Measures.

Competence	Methods for demonstrating competence
• Knowledge Requirement	• Evaluation Criteria
Proper usage of security equipment and systems, if any • Various types of security equipment and systems and their limitations, including those that could be used in case of attacks by pirates and armed robbers. • The need for testing, calibrating, and maintaining security systems and equipment, particularly whilst at sea.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Equipment and systems operations are carried out in accordance with established equipment operating instructions and taking into account the limitations of the equipment and systems. • Procedures and actions are in accordance with the principles established by the Maritime Security Measures.

Appendix 4.5 – Competency Matrix on Security Awareness for all Shipboard Personnel

Source: Section A-V1/6 of the STCW Code, as amended, August 2010

Competence • Basic Knowledge Requirement	Methods for demonstrating competence • Evaluation Criteria
Contribute to the enhancement of maritime security through heightened awareness • Maritime security terms and definitions including elements that may relate to piracy and armed robbery. • International maritime security policy and responsibilities of Governments, companies and persons. • Maritime security levels and their impact on security measures and procedures aboard ship and in port facilities. • Security reporting procedures. • Security-related contingency plans.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Requirements relating to enhanced maritime security are correctly identified.
Recognition of security threats • Techniques used to circumvent security measures. • Enabling recognition of potential security threats including elements that may relate to piracy and armed robbery. • Enabling recognition of weapons, dangerous substances, and devices and awareness of the damage they can cause. • Handling security-related information and security-related communications.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Maritime security threats are correctly identified.
Understanding of the need for and methods of maintaining security awareness and vigilance • Training, drill and exercise requirements under relevant conventions, codes and IMO circulars including those relevant for anti-piracy and anti-armed robbery.	**Assessment of evidence obtained from approved instruction or during attendance at an approved course** • Requirements relating to enhanced maritime security are correctly identified.

Source: MSC.1/Circ.1305, June 2009

1 Particulars of the ship and contact details

1.1 IMO Number*
1.2 Name of ship*
1.3 Port of registry*
1.4 Flag State*
1.5 Type of ship
1.6 Call Sign
1.7 Inmarsat call numbers (if available)
1.8 Gross Tonnage
1.9 Name of Company*
1.10 IMO Company identification number*
1.10 Name and 24-hour contact details of the Company Security Officer (or designated duty officer)

* no need to provide these details if a copy of the Continuous Synopsis record has been submitted

2 Port and port facility information

2.1 Port of arrival and port facility where the ship is to berth, if known
2.2 Expected date and time of arrival of the ship in port
2.3 Primary purpose of call

3 Information required by SOLAS regulation XI-2/9.2.1

3.1 The ship is provided with a valid:

 - International Ship Security Certificate ☐ Yes ☐ No

 - Interim International Ship Security Certificate ☐ Yes ☐ No

3.2 The certificate indicated in 3.1 has been issued by *<enter name of the Contracting Government* or the Recognized Security Organization*>* and which expires on *<enter date of expiry>*.

3.3 If the ship is not provided with a valid International Ship Security Certificate or a valid Interim International Ship Security Certificate, explain why

3.4 Does the ship have an approved ship security plan on board? ☐ Yes ☐ No

3.5 Current security level : ☐

3.6 Location of the ship at the time the report is made

3.7 List the last ten calls, in chronological order with the most recent call first, at port facilities at which the ship conducted ship/port interface together with the security level at which the ship operated:

189

| No.** | Date | | Port, Country, Port Facility and UNLOCODE (if available) | Security level |
	From	To		
10				
9				
8				
7				
6				
5				
4				
3				
2				
1				

*** Port of call No.10 is the last one before the port at which entry is being sought*

3.8   Did the ship, during the period specified in 3.7, take any special or additional security measures, beyond those specified in the approved ship security plan? ☐ Yes ☐ No

3.9   If the answer to 3.8 is YES, for each of such occasions please indicate the special or additional security measures which were taken by the ship:

No.	From	To	Special or additional security measures

3.10   List the ship-to-ship activities, in chronological order with the most recent ship-to-ship activity first, which have been carried out during the period specified in 3.7:

☐ Not applicable

No.	From	To	Location or Latitude and Longitude	Ship-to-ship activity

3.11   Have the ship security procedures, specified in the approved ship security plan, been maintained during each of the ship-to-ship activities specified in 3.10?   ☐ Yes ☐ No

3.12   If the answer to 3.11 is NO, identify the ship-to-ship activities for which the ship security procedures were not maintained and indicate, for each, the security measures which were applied in lieu:

No.	From	To	Security measures applied	Ship-to-ship activity

3.13   Provide a general description of cargo aboard the ship:

3.14   Is the ship carrying any dangerous substances (i.e. those covered by the International Maritime Dangerous Goods Code) as cargo?

☐ Yes ☐ No

3.15   If the answer to 3.14 is YES, provide details or attach a copy of the Dangerous Goods Manifest (IMO FAL Form 7)

3.16   A copy of the ship's Crew List (IMO FAL Form 5) is attached   ☐

3.17   A copy of the ship's Passenger List (IMO FAL Form 6) is attached ☐

4   Other security-related information

4.1   Is there any security-related matter you wish to report? ☐ Yes ☐ No

4.2   If the answer to 4.1 is YES, provide details (e.g. carriage of stowaways or persons rescued at sea)

5   Agent of the ship at the intended port of arrival

5.1   Name and contact details (telephone number) of the agent of the ship at the intended port of arrival:

6   Identification of the person providing the information

6.1   Name:

6.2   Title or position (Master, SSO, CSO or ship's Agent at intended port of arrival):

6.3   Signature:

This report is dated at *<enter place>* on *<enter time and date>*.

Appendix 4.7 – Example of a Ship Security Assessment and Plan Approval Process
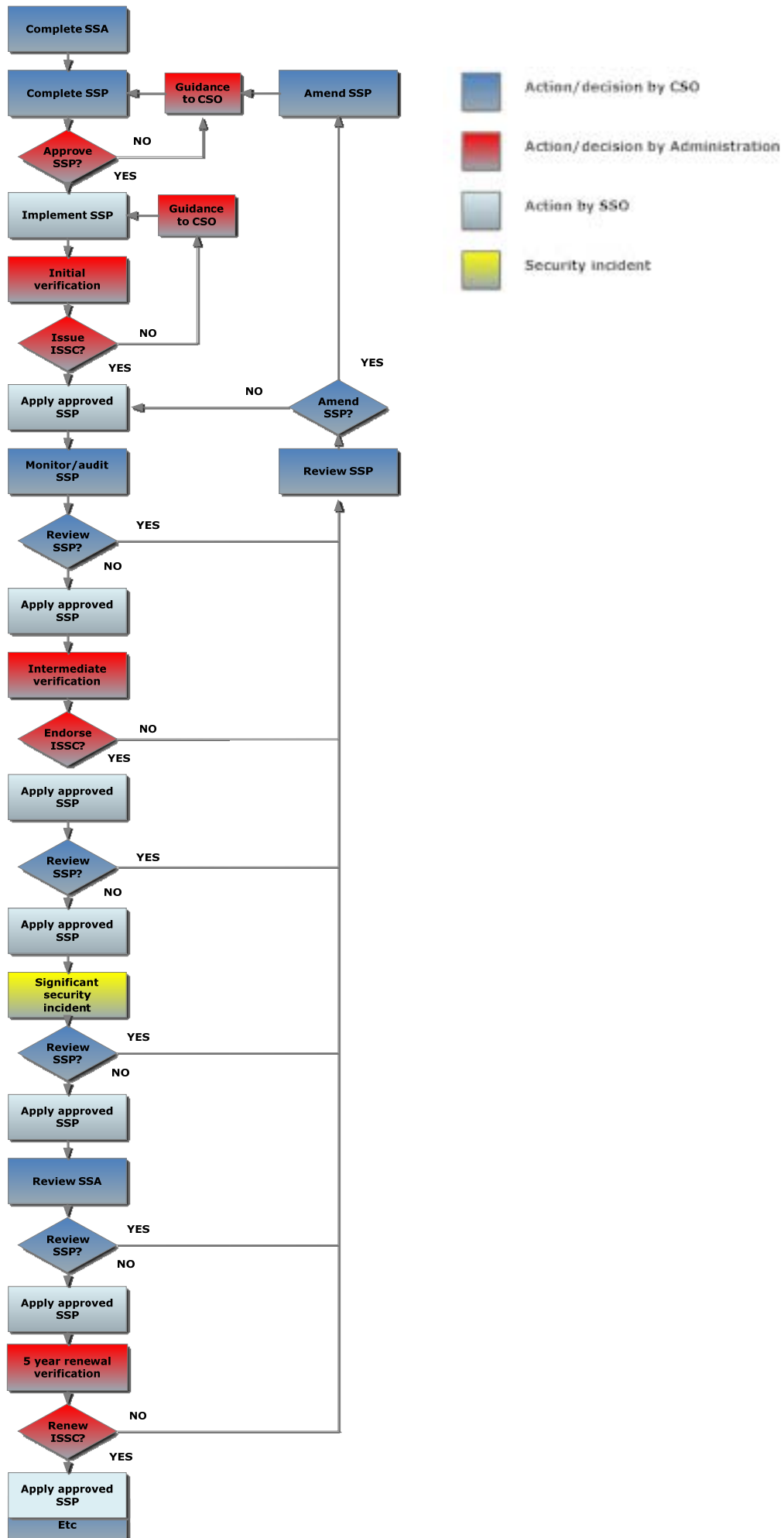
Complete SSA

Complete SSP ← **Guidance to CSO** ← **Amend SSP**

Approve SSP? — NO (to Guidance to CSO)
YES

Implement SSP ← **Guidance to CSO**

Initial verification

Issue ISSC? — NO
YES

Apply approved SSP ← NO — **Amend SSP?** — YES (to Amend SSP)

Monitor/audit SSP   **Review SSP**

Review SSP? — YES
NO

Apply approved SSP

Intermediate verification

Endorse ISSC? — NO
YES

Apply approved SSP

Review SSP? — YES
NO

Apply approved SSP

Significant security incident

Review SSP? — YES
NO

Apply approved SSP

Review SSA

Review SSP? — YES
NO

Apply approved SSP

5 year renewal verification

Renew ISSC? — NO
YES

Apply approved SSP

Etc

Legend:
- Action/decision by CSO
- Action/decision by Administration
- Action by SSO
- Security incident

192

1. Australian Government Department of Infrastructure and Transport, Guide to Preparing a Ship Security Plan, April 2009. Refer to: www.infrastructure.gov.au/transport/security/maritime/

This 29 page guide has been developed to provide ship operators covered by the Maritime Transport and Offshore Securities Act 2003 with a plan template so as to assist them with meeting all the requirements of an approved plan. It also contains a chart showing the plan approval process. Also, the template may be downloaded in WORD format.

2. United Kingdom, Department for Transport, Model Ship Security Plan, September 2008.

Refer to: www.dft.gov.uk/pgr/security/maritime

This 31 page document is a template showing CSOs and SSOs how to compile and submit their SSPs, including a four page template for the accompanying SSA Report. Also, the template may be downloaded in WORD format.

3. Commonwealth of Dominica Maritime Registry. Refer to: www.dominica-registry.com

This site provides access to the following 3 documents, including a plan template and a checklist both of which may be downloaded in WORD format:

- Model Ship Security Plan Guidance to accompany the Security Plan Template, last modified in June 2004. The 38 page document is in the form of 5 guides:
    - Guide 1 – Developing Threat Assessments
    - Guide 2 – Ship Initial Security Assessment (Survey)
    - Guide 3 – How to Identify and Mitigate Security Vulnerabilities
    - Guide 4 – Guidance for Establishing Protective Measures
    - Guide 5 – Developing Final Security Assessment

- Ship Security Plan Template, last modified July 2006. The 95 page template includes a SSO's Security Assessment Form as an appendix; and

- Aid for reviewing compliance for Ship Security Plans. The 15 page checklist was last modified in April 2008.

Appendix 4.9 – Implementation Checklist for Ship Security Personnel

Source: MSC.1/Circ.1193, May 2006

This checklist may be used by ship security personnel to examine the status of implementation of the Special Measures. The heading of each section is taken directly from paragraph A/7.2 of the ISPS Code.

Completion of the following section is recommended before using the checklist. It can be used to establish an overview of the ship's operations.

1. Company and Ship Overview

Name of Administration	
Name of company	
Name of ship	
IMO Ship identification number	
Name of CSO	
Name of SSO	
Number of ships operated by the company	
Number of ships for which the CSO is responsible	

2. Total manning of the ship and crew with security duties on board at the time of this assessment

Total number of crew members	
Number of crew with security duties	

3. Ship security information in the last 12 months

Number of crew members assigned on first time to the ship	
Number of different SSOs	
Number of changes in the security level	
Number of security incidents	
Number of breaches of security	

4. Security agreements and arrangements

Is the ship operating between port facilities covered by an alternative security agreement? If "Yes", provide relevant details.	
Has the ship implemented any equivalent security arrangements allowed by the Maritime Administration? If "Yes" provide relevant details.	
Is the ship operating under any temporary security measures? If "Yes", have these been approved or authorized by the Maritime Administration? If "Yes", provide relevant details.	

Guidance:

For each question, one of the 'Yes/No/Other' boxes should be ticked. Whichever one is used, the 'Comments' box provides space for amplification.

If the 'Yes' box is ticked, but the measures/procedures are not documented in the SSP, a short description of them should be included in the 'Comments' box. The 'Yes' box should be ticked only if all procedures and measures are in place. The 'Comments' box may also be used to indicate when procedures were last reviewed and measures tested (e.g. drills and exercises).

If the 'No' box is ticked, an explanation of why not should be included in the 'Comments' box along with details of any measures or procedures in place. Suggested actions should be recorded in the 'recommendations section at the end of the checklist.

If the 'other' box is ticked, a short description should be provided in the 'Comments' box (e.g. it could include instances where alternative measures/procedures or equivalent arrangements have been implemented). If the reason is due to the question not being applicable, then it should be recorded in the 'Comments' box as "not applicable".

If there is not enough space in the 'Comments' box, the explanation should be continued on a separate page (with the relevant question number, and in the case of questions with multiple options, the option added as a reference).

The 'Recommendations' boxes at the end of the checklist should be used to record any identified deficiencies and how these could be mitigated. A schedule for their implementation should be included.

The 'Outcomes' box at the end of the checklist should be used to provide a brief record of the assessment process. Along with the comments in the 'Recommendations' boxes, they form the basis for updating the SSP.

1. Ensuring the performance of all ship security duties

Part A	Yes	No	Other
.1 Does the ship's means of ensuring the performance of all security duties meet the requirements set out in the SSP for security levels 1 and 2? (ISPS Code, section A/7.2.1)	□	□	□
Comments:			
.2 Has the ship established measures to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship? (ISPS Code, section A/9.4.1)	□	□	□
Comments:			
.3 Has the ship established procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface? (ISPS Code, section A/9.4.4)	□	□	□
Comments:			
.4 Has the ship established procedures for responding to any security instructions Contracting Governments may give at security level 3? (ISPS Code, section A/9.4.5)	□	□	□
Comments:			
.5 Has the ship established procedures for evacuation in case of security threats or breaches of security? (ISPS Code, section A/9.4.6)	□	□	□
Comments:			
.6 Have the duties of shipboard personnel assigned security responsibilities and other shipboard personnel on security aspects been specified? (ISPS Code, section A/9.4.7)	□	□	□

Comments:			

	Yes	No	Other
.7 Have procedures been established for auditing the security activities of the ship? (ISPS Code, section A/9.4.8)	□	□	□
Comments:			

.8 Has the ship established procedures for interfacing with port facility security activities? (ISPS Code, section A/9.4.10)	□	□	□
Comments:			

.9 Have procedures been established for the periodic review of the ship security plan and for its updating? (ISPS Code, section A/9.4.11)	□	□	□
Comments:			

.10 Has the ship established procedures for reporting security incidents? (ISPS Code, section A/9.4.12)	□	□	□
Comments:			

Part B – Organization and performance of ship security duties	Yes	No	Other
.11 Has the ship implemented the organizational structure of security for the ships detailed in the SSP? (ISPS Code, paragraph B/9.2.1)	□	□	□
Comments:			

.12 Has the ship established the relationships with the Company, port facilities, other ships and relevant authorities with security responsibilities detailed in the SSP? (ISPS Code, paragraph B/9.2.2)	□	□	□
Comments:			

.13 Has the ship established the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities, detailed in the SSP? (ISPS Code, paragraph B/9.2.3)	□	□	□
Comments:			

.14 Has the ship implemented the basic security measures for security level 1, both operational and physical, that will always been in place, detailed in the SSP? (ISPS Code, paragraph B/9.2.4)	□	□	□

Comments:			

.15 Has the ship implemented the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3 detailed in the SSP? (ISPS Code, paragraph B/9.2.5)	□	□	□
Comments:			

.16 Has the ship established procedures for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances? (ISPS Code, paragraph B/9.2.6)	□	□	□
Comments:			

.17 Has the ship established reporting procedures to the appropriate Contracting Government's contact points? (ISPS Code, paragraph B/9.2.7)	□	□	□
Comments:			

.18 Has the ship established the duties and responsibilities of all shipboard personnel with a security role? (ISPS Code, paragraph B/9.7.1)	□	□	□
Comments:			

.19 Has the ship established the procedures or safeguards necessary to allow continuous communications to be maintained at all times? (ISPS Code, paragraph B/9.7.2)	□	□	□
Comments:			

.20 Has the ship established the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction? (ISPS Code, paragraph B/9.7.3)	□	□	□
Comments:			

.21 Has the ship established procedures and practices to protect security-sensitive information held in paper or electronic format? (ISPS Code, paragraph B/9.7.4)	□	□	□
Comments:			

.22 Has the ship established the type and maintenance requirements of security and surveillance equipment and systems, if any? (ISPS Code, paragraph B/9.7.5)	□	□	□

	Yes	No	Other
Comments:			

	Yes	No	Other
.23 Has the ship established the procedures to ensure timely submission and assessment of reports relating to possible breaches of security or security concerns? (ISPS Code, paragraph B/9.7.6)	□	□	□
Comments:			

	Yes	No	Other
.24 Has the ship put in place procedures to establish, maintain and update an inventory of any dangerous goods or hazardous substances carried on board, including their location? (ISPS Code, paragraph B/9.7.7)	□	□	□
Comments:			

2. Controlling access to the ship

Part A	Yes	No	Other
.1 Does the ship's means of controlling access to the ship meet the requirements set out in the SSP for security levels 1 and 2? (ISPS Code, section A/7.2.2)	□	□	□
Comments:			
.2 Has the ship established measures to prevent unauthorized access? (ISPS Code, section A/9.4.3)	□	□	□
Comments:			

Part B − Access to the ship	Yes	No	Other
.3 Has the ship established security measures covering all means of access to the ship identified in the SSA? (ISPS Code, paragraph B/9.9)			
A. Access ladders	□	□	□
B. Access gangways	□	□	□
C. Access ramps	□	□	□
D. Access doors, side scuttles, windows and ports	□	□	□
E. Mooring lines and anchor chains	□	□	□
F. Cranes and hoisting gear	□	□	□
Comments:			

	Yes	No	Other
4 Has the ship identified appropriate locations where access restrictions or prohibitions should be applied for each of the security levels? (ISPS Code, paragraph B/9.10)	□	□	□

Comments:			

.5 Has the ship established for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge? (ISPS Code, paragraph B/9.11)			
A. Security level 1	□	□	□
B. Security level 2	□	□	□
C. Security level 3	□	□	□
Comments:			

.6 Has the ship established the frequency of application of any access controls? (ISPS Code, paragraph B/9.13)	□	□	□
Comments:			

Security level 1

.7 Has the ship established security measures to check the identity of all persons seeking to board the ship and confirming their reasons for doing so? (ISPS Code, paragraph B/9.14.1)	□	□	□
Comments:			

.8 Has the ship established procedures to liaise with the port facility to ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry-on items), personal effects, vehicles and their contents can take place? (ISPS Code, paragraph B/9.14.2)	□	□	□
Comments:			

.9 Has the ship identified access points that should be secured or attended to prevent unauthorized access? (ISPS Code, paragraph B/9.14.6)	□	□	□
Comments:			

.10 Has the ship established security measures to secure, by locking or other means, access to unattended spaces, adjoining areas to which passengers and visitors have access? (ISPS Code, paragraph B/9.14.7)	□	□	□
Comments:			

.11 Has the ship provided security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance? (ISPS Code, paragraph B/9.14.8)	□	□	□

Comments:			

.12 Has the ship established the frequency of searches, including random searches, of all those seeking to board the ship? (ISPS Code, paragraph B/9.15)	□	□	□
Comments:			

Security level 2

.13 Has the ship limited the number of access points to the ship, identifying those to be closed and the means for adequately securing them? (ISPS Code, paragraph B/9.16.2)	□	□	□
Comments:			

.14 Has the ship established a restricted area on the shore side of the ship, in close co-operation with the port facility? (ISPS Code, paragraph B/9.16.4)	□	□	□
Comments:			

.15 Has the ship arrangements to escort visitors on the ship? (ISPS Code, paragraph B/9.16.6)	□	□	□
Comments:			

.16 Has the ship provided additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance? (ISPS Code, paragraph B/9.16.7)	□	□	□
Comments:			

.17 Has the ship established procedures for carrying out a full or partial search of the ship? (ISPS Code, paragraph B/9.16.8)	□	□	□
Comments:			

3. Controlling the embarkation of persons and their effects

Part A	Yes	No	Other
.1 Does the ship's measures for controlling the embarkation of persons and their effects meet the requirements set out in the SSP for security levels 1 and 2? (ISPS Code, section A/7.2.3)	□	□	□
Comments:			

Part B – Access to the ship	Yes	No	Other
Security level 1			
.2 Has the ship established procedures to liaise with the port facility to ensure that vehicles destined to be loaded onboard car carriers, ro-ro and other passenger ships are subjected to search prior to loading? (ISPS Code, paragraph B/9.14.3)	□	□	□
Comments:			
.3 Has the ship established security measures to segregate checked persons and their personal effects from unchecked persons and their personal effects? (ISPS Code, paragraph B/9.14.4)	□	□	□
Comments:			
.4 Has the ship established security measures to segregate embarking from disembarking passengers? (ISPS Code, paragraph B/9.14.5)	□	□	□
Comments:			

Security level 2

	Yes	No	Other
.5 Has the ship increased the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship? (ISPS Code, paragraph B/9.16.5)	□	□	□
Comments:			

Part B – Handling unaccompanied baggage (ISPS Code, paragraphs B/9.38 to B/9.40)	Yes	No	Other
.6 Has the ship established security measures to be applied to ensure that unaccompanied baggage is identified and subject to appropriate screening, including searching, before it is accepted on board? (ISPS Code, paragraph B/9.38)	□	□	□
Comments:			

Security level 1

	Yes	No	Other
.7 Has the ship established security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100%, which may include use of x-ray screening? (ISPS Code, paragraph B/9.39)	□	□	□
Comments:			

Security level 2

201

	Yes	No	Other
.8 Has the ship established additional security measures to be applied when handling unaccompanied baggage, which should include 100% x-ray screening of all unaccompanied baggage? (ISPS Code, paragraph B/9.40)	□	□	□
Comments:			

4.   Monitoring of restricted areas

Part A	Yes	No	Other
.1 Does the ship's measures for monitoring access to restricted areas, to ensure that only authorized persons have access, meet the requirements set out in the SSP for security levels 1 and 2? (ISPS Code, sections A/7.2.4 and A/7.3)	□	□	□
Comments:			

	Yes	No	Other
.2 Have restricted areas been identified and measures put in place to prevent unauthorized access to them? (ISPS Code, section A/9.4.2)	□	□	□
Comments:			

Part B – Restricted areas on the ship	Yes	No	Other
.3 Has the ship clearly established policies and practices to control access to all restricted areas? (ISPS Code, paragraph B/9.19)	□	□	□
Comments:			

	Yes	No	Other
.4 Has the ship clearly marked all restricted areas, indicating that access to the area is restricted and that unauthorized presence in the area constitutes a breach of security? (ISPS Code, paragraph B/9.20)	□	□	□
Comments:			

.5 Which of the following have been identified as restricted areas? (ISPS Code, paragraph B/9.21)			
A. Navigation bridge, machinery spaces of category A and other control stations	□	□	□
B. Spaces containing security and surveillance equipment and systems and their controls and lighting system controls	□	□	□
C. Ventilation and air-conditioning systems and other similar spaces	□	□	□
D. Spaces with access to potable water tanks, pumps and manifolds	□	□	□
E. Spaces containing dangerous goods or hazardous substances	□	□	□
F. Spaces containing cargo pumps and their controls	□	□	□
G. Cargo spaces and spaces containing ship's stores	□	□	□
H. Crew accommodation	□	□	□

I. Any other areas	□	□	□
Comments:			

Security level 1

.6 Which of the following security measures have be applied to restricted areas on the ship? (ISPS Code, paragraph B/9.22)			
A. Locking or securing access points	□	□	□
B. Using surveillance equipment to monitor the areas	□	□	□
C. Using guards or patrols	□	□	□
D. Using automatic intrusion-detection devices to alert the ship's personnel of unauthorized access	□	□	□
Comments:			

Security level 2

.7 Which of the following additional security measures have be applied to restricted areas on the ship? (ISPS Code, paragraph B/9.23)			
A. Establishing restricted areas adjacent to access points	□	□	□
B. Continuously monitoring surveillance equipment	□	□	□
C. Dedicating additional personnel to guard and patrol restricted areas	□	□	□
Comments:			

5.   Monitoring of deck areas and areas surrounding the ship

Part A	Yes	No	Other
.1 Does the ship's means of monitoring deck areas and areas surrounding the ship meet the requirements identified in the SSP for security levels 1 and 2? (ISPS Code, section A/7.2.5)	□	□	□
Comments:			

Part B – Access to the ship	Yes	No	Other

Security level 2

.2 Has the ship assigned additional personnel to patrol deck areas during silent hours to deter unauthorized access? (ISPS Code, paragraph B/9.16.1)	□	□	□
Comments:			

	Yes	No	Other
.3 Has the ship established security measures to deter waterside access to the ship including, for example, in liaison with the port facility, provision of boat patrols? (ISPS Code, paragraph B/9.16.3)	□	□	□
Comments:			

Part B – Monitoring the security of the ship (ISPS Code, paragraphs B/9.42 to B/9.48)	**Yes**	**No**	**Other**
.4 Which of the following monitoring capabilities have been established by the ship to monitor the ship, the restricted areas on board and areas surrounding the ship? (ISPS Code, paragraph B/9.42)			
A. Lighting	□	□	□
B. Watchkeepers, security guards and deck watches, including patrols	□	□	□
C. Automatic intrusion-detection devices and surveillance equipment	□	□	□
Comments:			

	Yes	No	Other
.5 Do any automatic intrusion-detection devices on the ship activate an audible and/or visual alarm at a location that is continuously attended or monitored? (ISPS Code, paragraph B/9.43)	□	□	□
Comments:			

	Yes	No	Other
.6 Has the ship established the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or power disruptions? (ISPS Code, paragraph B/9.44)	□	□	□
Comments:			

Security level 1

	Yes	No	Other
.7 Has the ship established the security measures to be applied, which may be a combination of lighting, watchkeepers, security guards or the use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular? (ISPS Code, paragraph B/9.45)	□	□	□
Comments:			

	Yes	No	Other
.8 Are the ship's deck and access points illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage? (ISPS Code, paragraph B/9.46)	□	□	□
Comments:			

Security level 2

.9 Which of the following additional security measures have been established to enhance monitoring and surveillance activities? (ISPS Code, paragraph B/9.47)			
A. Increasing the frequency and detail of security patrols	□	□	□
B. Increasing the coverage and intensity of lighting or the use of security and surveillance equipment	□	□	□
C. Assigning additional personnel as security look-outs	□	□	□
D. Ensuring co-ordination with water-side boat patrols, and foot or vehicle patrols on the shore side, when provided	□	□	□
Comments:			

6. Supervising the handling of cargo and ship's stores

Part A	Yes	No	Other
.1 Does the ship's means of supervising the handling of:			
A. cargo	□	□	□
B. ship's stores meet the requirements identified in the SSP at security levels 1 and 2? (ISPS Code, section A/7.2.6)	□	□	□
Comments:			

Part B – Handling of cargo	Yes	No	Other

Security level 1

.2 Are measures employed to routinely check the integrity of cargo, including the checking of seals, during cargo handling? (ISPS Code, paragraphs B/9.27.1 and B/9.27.4)	□	□	□
Comments:			

.3 Are measures employed to routinely check cargo being loaded matches the cargo documentation? (ISPS Code, paragraph B/9.27.2)	□	□	□
Comments:			

.4 Does the ship ensure, in liaison with the port facility, that vehicles to be loaded on car carriers, ro-ro and passenger ships are searched prior to loading, in accordance with the frequency required in the SSP? (ISPS Code, paragraph B/9.27.3)	□	□	□
Comments:			

.5 Which of the following security measures are employed during cargo checking? (ISPS Code, paragraph B/9.28)			
A. Visual examination	□	□	□
B. Physical examination	□	□	□

C. Scanning or detection equipment	□	□	□
D. Other mechanical devices	□	□	□
E. Dogs	□	□	□
Comments:			

Security level 2

.6 Which of the following additional security measures are applied during cargo handling? (ISPS Code, paragraph B/9.30)			
A. Detailed checking of cargo, cargo transport units and cargo spaces	□	□	□
B. Intensified checks to ensure that only the intended cargo is loaded	□	□	□
C. Intensified searching of vehicles	□	□	□
D. Increased frequency and detail in checking of seals or other methods used to prevent tampering	□	□	□
Comments:			

Part B – Delivery of ship's stores (ISPS Code, paragraphs B/9.33 to B/9.36)	Yes	No	Other
.7 Has the ship established security measures to ensure stores being delivered match the order, prior to being loaded on board and to ensure their immediate secure stowage at security level 1? (ISPS Code, paragraph B/9.35)	□	□	□
Comments:			
.8 Has the ship established additional security measures at security level 2 by exercising checks prior to receiving stores on board and intensifying inspections? (ISPS Code, paragraph B/9.36)	□	□	□
Comments			

7. Ensuring security communication is readily available

Part A	Yes	No	Other
.1 Do the ship's communication equipment and procedures meet the requirements identified in the SSP at security levels 1 and 2? (ISPS Code, section A/7.2.7)	□	□	□
Comments:			
.2 Has the ship security officer been identified? (ISPS Code, section A/9.4.13)	□	□	□
Comments:			

	Yes	No	Other
.3 Has the company security officer been identified and 24 hour contact details been provided? (ISPS Code, section A/9.4.14)	□	□	□
Comments:			

	Yes	No	Other
.4 Has the ship established procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board? (ISPS Code, section A/9.4.15)	□	□	□
Comments:			

	Yes	No	Other
.5 Has the frequency for testing or calibration of any security equipment provided on board been specified? (ISPS Code, section A/9.4.16)	□	□	□
Comments:			

	Yes	No	Other
.6 Have the locations on the ship where the ship security alert system activation points are provided been identified? (ISPS Code, section A/9.4.17)	□	□	□
Comments:			

	Yes	No	Other
.7 Have procedures, instructions and guidance been established and communicated on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts? (ISPS Code, section A/9.4.18)	□	□	□
Comments:			

8. Training, Drills and Exercises

Part A	Yes	No	Other
.1 Have the:			
A. CSO and appropriate shore-based personnel security personnel received sufficient training to perform their assigned duties? (ISPS Code, section A.13.1)	□	□	□
B. SSO received sufficient training to perform their assigned duties? (ISPS Code, section A/13.2)	□	□	□
Comments:			

	Yes	No	Other
.2 Do shipboard personnel having specific security duties and responsibilities understand their responsibilities for ship security and have sufficient knowledge and ability to perform their assigned duties? (ISPS Code, section A/13.3)	□	□	□
Comments:			

	Yes	No	Other
.3 Has the company and ship implemented drills and participated in exercises? (ISPS Code, sections A/13.4 and A/13.5)	□	□	□

207

Comments:			

	Yes	No	Other
.4 Has the ship established procedures for training, drills and exercises associated with the ship security plan? (ISPS Code, section A/9.4.9)	□	□	□
Comments:			

Part B − Training, drills, and exercises on ship security	Yes	No	Other
.5 Have the CSO, appropriate shore-based Company personnel and the SSO received the appropriate levels of training? (ISPS Code, paragraphs B/13.1, B/13.2)	□	□	□
Comments:			

	Yes	No	Other
.6 Do shipboard personnel with security responsibilities have sufficient knowledge and ability to perform their duties? (ISPS Code, paragraph B/13.3)	□	□	□
Comments:			

.7 Are security drills conducted:			
A. at least every three months?	□	□	□
B. in cases where more than 25% of the ship's personnel has been changed, at any one time, with personnel that have not previously participated in any drill on that ship within the last three months? (ISPS Code, paragraph B/13.6)	□	□	□
C. to test individual elements of the ship security plan such as those security threats listed in ISPS Code, paragraph B/8.9? (ISPS Code, paragraph B/13.6)	□	□	□
Comments:			

9.   Miscellaneous

Part A	Yes	No	Other
.1 Have different RSOs undertaken (a) the preparation of the SSA and SSP and (b) the review and approval of the SSP? (ISPS Code, section A/9.2.1)	□	□	□
Comments:			

	Yes	No	Other
.2 Has the Master a contact point in the Administration to seek consent for the inspection of those provisions in the SSP that are considered confidential information, when access to them is requested by a duly authorized officer of another Contracting Government? (ISPS Code, section A/9.8.1)	□	□	□
Comments:			

.3 Has the ship established procedures to protect from unauthorized access or disclosure the records of activities addressed in the SSP which are required to be kept on board? (ISPS Code, section A/10.4)	☐	☐	☐
Comments:			

.4 In which of the following circumstances does the ship request completion of a Declaration of Security (DoS)? (ISPS Code, section A/5.2)			
A. When the ship is operating at a higher security level than the port facility or another ship it is interfacing with	☐	☐	☐
B. The ship is covered by an agreement on a DoS between Contracting Governments	☐	☐	☐
C. When there has been a security threat or a security incident involving the ship or port facility it is calling at	☐	☐	☐
D. When the ship is at a port which is not required to have and implement an approved port facility security plan	☐	☐	☐
E. When the ship is conducting ship-to-ship activities with another ship not required to have and implement an approved SSP	☐	☐	☐
Comments:			

.5 Does the CSO or SSO periodically review the SSA for accuracy as part of the SSP review process? (ISPS Code, section A/10.1.7)	☐	☐	☐
Comments:			

.6 Does the ship adequately maintain the required security records and are they sufficiently detailed to allow the CSO and SSO to identify areas for improvement or change in the current security procedures and measures? (ISPS Code, section A/10.1)			
A. Training, drills and exercises (ISPS Code, section A/10.1.1)	☐	☐	☐
B. Security threats and security incidents (ISPS Code, section A/10.1.2)	☐	☐	☐
C. Breaches of security (ISPS Code, section A/10.1.3)	☐	☐	☐
D. Periodic review of the SSP (ISPS Code, section A/10.1.8)	☐	☐	☐
Comments:			

.7 Is the ship adequately manned and its complement includes the grades/capacities and number of persons required for the safe operation and the security of the ship and for the protection of the marine environment (IMO Assembly resolution A.890(21) as amended by Assembly resolution A.955(23), SOLAS regulation V/14.1 and ISPS Code, paragraph B/4.28)			
A. When the ship is operating at security level 1	☐	☐	☐
B. When the ship is operating at security level 2	☐	☐	☐
Comments:			

209

Part B – Miscellaneous	Yes	No	Other
.8 Has the ship established procedures on handling requests for a Declaration of Security from a port facility? (ISPS Code, paragraph B/9.52)	☐	☐	☐
Comments:			

	Yes	No	Other
.9 Have procedures been established in the SSP as to how the CSO and SSO intend to audit the continued effectiveness of the SSP and to review, update or amend the SSP? (ISPS Code, paragraph B/9.53)	☐	☐	☐
Comments:			

	Yes	No	Other
.10 Has the ship established additional security procedures to be implemented when calling into a port facility which is not required to comply with the requirements of SOLAS chapter XI-2 and the ISPS Code? (ISPS Code, paragraph B/4.20)	☐	☐	☐
Comments:			

Recommendations

This section should be used to record any deficiencies identified by the checklist and how these could be mitigated. In essence this will provide an action plan for the CSO and/or SSO.

Recommendations/For Action: Section 1: Ensuring the performance of all ship security duties.

Recommendations/For Action: Section 2: Controlling access to the ship.

Recommendations/For Action: Section 3: Controlling the embarkation of persons and their effects.

Recommendations/For Action: Section 4: Monitoring of restricted areas.

Recommendations/For Action: Section 5: Monitoring of deck areas and areas surrounding the ship.

Recommendations/For Action: Section 6: Supervising the handling of cargo and ship's stores.

Recommendations/For Action: Section 7: Ensuring security communication is readily available.

Recommendations/For Action: Section 8: Training, drills and exercises.

Recommendations/For Action: Section 9: Miscellaneous.

OUTCOMES

This section should be used to record the findings of the voluntary self-assessment and any other issues arising. These findings could be raised with ship or company personnel or be used as the basis to seek guidance from the Administration, as appropriate.

Signature of assessor	**Date of completion:**
Name	**Title**
....	....

211

Appendix 4.10 – Implementation Checklist for Shipping Companies & their CSOs

Source: MSC.1/Circ. 1217, December 2006

This checklist may be used by shipping companies and their CSOs to assess the status of implementation of the Maritime Security Measures within their company and on the ships that they operate.

Completion of the following section is recommended before using the checklist. It can be used to establish an overview of company operations.

Company Name	
Company Address	
CSO Name(s)	

Complete separate table for each CSO as appropriate

Name of CSO	
Does the CSO hold an appropriate training certificate?	
Was this certificate submitted to the Administration for recognition?	

List of ship(s)

Name of ship	IMO Number	Type	Flag	SSP approved by, on	ISSC issued by, on
1)					
2)					
3)					
4)					
5)					
6)					
7)					
8)					
9)					
10)					

Guidance:

For each question, one of the 'Yes/No/Other' boxes should be ticked. Whichever one is used, the 'Comments' box provides space for amplification.

If the 'Yes' box is ticked, but the measures/procedures are not documented in the SSP, a short description of them should be included in the 'Comments' box. The 'Yes' box should be ticked only if all procedures and measures are in place. The 'Comments' box may also be used to indicate when procedures were last reviewed and measures tested (e.g. drills and exercises).

If the 'No' box is ticked, an explanation of why not should be included in the 'Comments' box along with details of any measures or procedures in place. Suggested actions should be recorded in the 'recommendations section at the end of the checklist.

If the 'other' box is ticked, a short description should be provided in the 'Comments' box (e.g. it could include instances where alternative measures/procedures or equivalent arrangements have been implemented). If the reason is due to the question not being applicable, then it should be recorded in the 'Comments' box as "not applicable".

If there is not enough space in the 'Comments' box, the explanation should be continued on a separate page (with the relevant question number, and in the case of questions with multiple options, the option added as a reference).

The 'Recommendations' boxes at the end of the checklist should be used to record any identified deficiencies and how these could be mitigated. A schedule for their implementation should be included.

The 'Outcomes' box at the end of the checklist should be used to provide a brief record of the assessment process. Along with the comments in the 'Recommendations' boxes, they form the basis for updating the SSP.

1. Continuous Synopsis Record (CSR) (SOLAS regulation XI-1/5)

	Yes	No	Other
.1 Has the Company ensured that all of its ships have been issued with an up-to-date CSR? (SOLAS regulation XI-1/5)	□	□	□
Comments:			

	Yes	No	Other
.2 Has the Company ensured that procedures are in place to notify the Administration when ships are transferred to the flag of another State? (SOLAS regulation XI-1/5.7)	□	□	□
Comments:			

2. Ship security alert system (SSAS) (SOLAS regulation XI-2/6)

	Yes	No	Other
.1 Has the Company ensured that an SSAS has been installed and that it operates as required? (SOLAS regulations XI-2/6.1 and XI-2/6.3)	□	□	□
Comments:			

	Yes	No	Other
.2 Has the Company been designated by each ship's Administration to receive ship-to-shore security alerts (a separate answer should be given for each flag under which the Company's ships are flying)? (SOLAS regulation XI-2/6.2.1)	□	□	□

Comments:			

	Yes	No	Other
.3 Does the CSO inform the Administration of SSAS implementation details and alterations? (SOLAS regulation XI-2/6.2.1)	□	□	□
Comments:			

	Yes	No	Other
.4 Does the Company have procedures in place to act upon receipt of a ship-to-shore security alert, including notification of the Administration? (SOLAS regulation XI-2/6.2.1)	□	□	□
Comments:			

3.   **Master's discretion for ship safety and security (SOLAS regulation XI-2/8.1)**

	Yes	No	Other
.1 Has the Company adopted a clearly stated policy that nothing constrains the master from taking or executing any decision which in his professional judgement is necessary to maintain the safety and security of the ship? (SOLAS regulation XI-2/8.1)	□	□	□
Comments:			

4.   **Obligations of the Company (SOLAS regulation XI-2/5, ISPS Code, sections A/6.1, A/6.2 and paragraphs B/6.1 to B/6.6)**

	Yes	No	Other
.1 Has the Company ensured that the master has available on board, at all times, information through which officers duly authorised by a Contracting Government can establish the following: (SOLAS regulation XI-2/5)			
.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?	□	□	□
.3 In cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies)?	□	□	□
Comments:			

	Yes	No	Other
.2 Has the Company established in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary? (ISPS Code, section A/6.1)	□	□	□

	Yes	No	Other
Comments:			

	Yes	No	Other
.3 Has the Company ensured that the CSO, the master and the ship security officer (SSO) are being given the necessary support to fulfil their duties and responsibilities in accordance with SOLAS chapter XI-2 and Part A of the Code? (ISPS Code, section A/6.2)	□	□	□
Comments:			

Part B – Obligations of the Company (ISPS Code, paragraphs B/6.1 to B/6.6)

	Yes	No	Other
.4 Has the Company provided the master of each ship with information to meet the requirements of the Company under the provisions of SOLAS regulation XI-2/5, for each of the following (ISPS Code, paragraph B/6.1)			
.1 Parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, and concessionaries (for example, retail sales outlets, casinos, etc.)?	□	□	□
.2 Parties responsible for deciding the employment of the ship, including time or bareboat charterer(s) or any other entity acting in such capacity?	□	□	□
.3 In cases when the ship is employed under the terms of a charter party, the contact details of those parties, including time or voyage charterers?	□	□	□
Comments:			

	Yes	No	Other
.5 Does the Company update and keep the information provided current as and when changes occur? (ISPS Code, paragraph B/6.2)	□	□	□
Comments:			

	Yes	No	Other
.6 Is the information provided in the English, French or Spanish language? (ISPS Code, paragraph B/6.3)	□	□	□
Comments:			

	Yes	No	Other
.7 If the ships were constructed before 1 July 2004, does this information reflect the actual condition on that date? (ISPS Code, paragraph B/6.4)	□	□	□
Comments:			

	Yes	No	Other
.8 If the ships were constructed on or after 1 July 2004, or the ships were constructed before 1 July 2004 but were out of service on 1 July 2004, was the information provided as from the date of entry of the ship into service and does it reflect the actual condition on that date? (ISPS Code, paragraph B/6.5)	□	□	□

Comments:			

	Yes	No	Other
.9　When a ship is withdrawn from service, is the information provided as from the date of re-entry of the ship into service and does it reflect the actual condition on that date? (ISPS Code, paragraph B/6.6)	□	□	□
Comments:			

5.　Control and compliance measures (SOLAS regulation XI-2/9.2.1)

	Yes	No	Other
.1　Does the Company provide, or has it ensured that its ships provide, confirmation to a Contracting Government, on request, of the information required in SOLAS regulation XI-2/9.2.1.1 to 9.2.1.6, using the standard data set detailed in MSC/Circ.1305 (SOLAS regulation XI-2/9.2.1)	□	□	□
Comments:			

6.　Verification and certification for ships (ISPS Code, section A/19)

Part A	Yes	No	Other
.1　Does the Company ensure that each ship to which SOLAS chapter XI-2 and the ISPS Code apply is covered by a valid International Ship Security Certificate (ISSC)? (ISPS Code, section A/19)	□	□	□
Comments:			
.2　Does the Company ensure that, when it assumes responsibility for a ship not previously operated by that Company, the existing ISSC is no longer used? (ISPS Code, section A/19.3.9.2)	□	□	□
Comments:			
.3　Does the Company, when it ceases to be responsible for the operation of a ship, transmit to the receiving Company as soon as possible, copies of any information related to the or to facilitate the verifications required for an ISSC to be issued, as described in the ISPS Code, section A/19.4.2? (ISPS Code, section A/19.3.9.2)	□	□	□
Comments:			

7. Ship security assessment (ISPS Code, sections A/8.1 to A/8.5)

	Yes	No	Other
.1 Does the CSO ensure that each ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship? (ISPS Code, sections A/2.1.7 and A/8.2 and paragraphs B/8.1 and B/8.4)	□	□	□
Comments:			

	Yes	No	Other
.2 Does the CSO ensure that the persons carrying out the ship security assessment take into account the guidance given in Part B of the ISPS Code and, in particular, paragraphs B/8.2 to B/8.13 see Part B below)? (ISPS Code, section A/8.2 and paragraph B/8.1)	□	□	□
Comments:			

	Yes	No	Other
.3 Does the CSO ensure that ship security assessments include an on-scene security survey and at least the following elements: (ISPS Code, section A/8.4)			
.1 Identification of existing security measures, procedures and operations?	□	□	□
.2 Identification and evaluation of key shipboard operations that it is important to protect?	□	□	□
.3 Identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures?	□	□	□
.4 Identification of weaknesses, including human factors, in the infrastructure, policies and procedures?	□	□	□
Comments:			

	Yes	No	Other
.4 Are ship security assessments documented, reviewed, accepted and retained by the Company? (ISPS Code, section A/8.5)	□	□	□
Comments:			

Part B – CSO requirements to conduct an assessment (ISPS Code, paragraphs B/8.2 and B/8.5)

	Yes	No	Other
.5 Has the CSO ensured that, prior to commencing the SSA, advantage was taken of information available on the assessment of threat for the ports at which the ship would call or at which passengers would embark or disembark and about the port facilities and their protective measures? (ISPS Code, paragraph B/8.2)	□	□	□
Comments:			

	Yes	No	Other
.6 Has the CSO studied previous reports on similar security needs? (ISPS Code, paragraph B/8.2)	□	□	□
Comments:			

.7 Has the CSO met with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment? (ISPS Code, paragraph B/8.2)	□	□	□
Comments:			

.8 Has the CSO followed any specific guidance offered by the Contracting Governments? (ISPS Code, paragraph B/8.2)	□	□	□
Comments:			

.9 Does the CSO obtain and record the information required to conduct an assessment, including the following: (ISPS Code, paragraph B/8.5)			
.1 The general layout of the ship?	□	□	□
.2 The location of areas which should have restricted access such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc?	□	□	□
.3 The location and function of each actual or potential access point to the ship?	□	□	□
.4 Changes in the tide which may have an impact on the vulnerability or security of the ship?	□	□	□
.5 The cargo spaces and stowage arrangements?	□	□	□
.6 The locations where ship's stores and essential maintenance equipment is stored?	□	□	□
.7 The locations where unaccompanied baggage is stored?	□	□	□
.8 The emergency and stand-by equipment available to maintain essential services?	□	□	□
.9 The number of ship's personnel and existing security duties and any existing training requirement practices of the Company?	□	□	□
.10 Existing security and safety equipment for the protection of passengers and ship's personnel?	□	□	□
.11 Escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship?	□	□	□
.12 Existing agreements with private security companies providing ship/water-side security services?	□	□	□
.13 Existing security measures and procedures in effect, including inspection and control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems?	□	□	□
Comments:			

Part B – Content of the SSA (ISPS Code, paragraphs B/8.3, B/8.4, B/8.6 to B/8.13)

.10 Does the CSO ensure that the ship security assessments address the following			

elements on board or within the ship: (ISPS Code, paragraph B/8.3)			
.1 Physical security?	☐	☐	☐
.2 Structural integrity?	☐	☐	☐
.3 Personnel protection systems?	☐	☐	☐
.4 Procedural policies?	☐	☐	☐
.5 Radio and telecommunication systems, including computer systems and networks?	☐	☐	☐
.6 Other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility?	☐	☐	☐
Comments:			

.11 Does the CSO ensure that those involved in conducting a ship security assessment are able to draw upon expert assistance in relation to the following: (ISPS Code, paragraph B/8.4)			
.1 Knowledge of current security threats and patterns?	☐	☐	☐
.2 Recognition and detection of weapons, dangerous substances and devices?	☐	☐	☐
.3 Recognition, on a non-discriminatory basis, of characteristics and behaviour patterns of persons who are likely to threaten security?	☐	☐	☐
.4 Techniques used to circumvent security measures?	☐	☐	☐
.5 Methods used to cause a security incident?	☐	☐	☐
.6 Effects of explosives on ship's structures and equipment?	☐	☐	☐
.7 Ship security?	☐	☐	☐
.8 Ship/port interface business practices?	☐	☐	☐
.9 Contingency planning, emergency preparedness and response?	☐	☐	☐
.10 Physical security?	☐	☐	☐
.11 Radio and telecommunication systems, including computer systems and networks?	☐	☐	☐
.12 Marine engineering?	☐	☐	☐
.13 Ship and port operations?	☐	☐	☐
Comments:			

.12 Does the CSO ensure that ship security assessments examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security? This includes points of access as well as those who seek to obtain unauthorized entry. (ISPS Code, paragraph B/8.6)	☐	☐	☐
Comments:			

.13 Does the CSO ensure that ship security assessments consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions, and have determined security guidance including the following: (ISPS Code, paragraph B/8.7)			
.1 The restricted areas?	☐	☐	☐

.2 The response procedures to fire or other emergency conditions?	□	□	□
.3 The level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc?	□	□	□
.4 The frequency and effectiveness of security patrols?	□	□	□
.5 The access control systems, including identification systems?	□	□	□
.6 The security communications systems and procedures?	□	□	□
.7 The security doors, barriers and lighting?	□	□	□
.8 The security and surveillance equipment and systems, if any?	□	□	□
Comments:			

.14 Does the CSO ensure that ship security assessments consider the persons, activities, services and operations that it is important to protect, which includes the following: (ISPS Code, paragraph B/8.8)			
.1 The ship's personnel?	□	□	□
.2 Passengers, visitors, vendors, repair technicians, port facility personnel, etc?	□	□	□
.3 The capacity to maintain safe navigation and emergency response?	□	□	□
.4 The cargo, particularly dangerous goods or hazardous substances?	□	□	□
.5 The ship's stores?	□	□	□
.6 The ship's security communication equipment and systems, if any?	□	□	□
.7 The ship's security surveillance equipment and systems, if any?	□	□	□
Comments:			

.15 Does the CSO ensure that ship security assessments consider all possible threats, which may include the following types of security incidents: (ISPS Code, paragraph B/8.9)			
.1 Damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism?	□	□	□
.2 Hijacking or seizure of the ship or of persons on board?	□	□	□
.3 Tampering with cargo, essential ship equipment or systems or ship's stores?	□	□	□
.4 Unauthorized access or use including presence of stowaways?	□	□	□
.5 Smuggling weapons or equipment, including weapon of mass destruction?	□	□	□
.6 Use of the ship to carry those intending to cause a security incident and/or their equipment?	□	□	□
.7 Use of the ship itself as a weapon or as a means to cause damage or destruction?	□	□	□
.8 Attacks from seaward whilst at berth or at anchor?	□	□	□
.9 Attacks whilst at sea?	□	□	□
Comments:			

.16 Does the CSO ensure that ship security assessments take into account all			

possible vulnerabilities, which may include the following: (ISPS Code, paragraph B/8.10)			
.1 Conflicts between safety and security measures?	□	□	□
.2 Conflicts between shipboard duties and security assignments?	□	□	□
.3 Watchkeeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance?	□	□	□
.4 Any identified security training deficiencies?	□	□	□
.5 Any security equipment and systems, including communication systems?	□	□	□
Comments:			

.17 Do the CSO and the SSO always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods? (ISPS Code, paragraph B/8.11)	□	□	□
Comments:			

.18 Does the CSO ensure that, upon completion of the SSA, a report is prepared consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability? Is this report protected from unauthorized access or disclosure? (ISPS Code, paragraph B/8.12)	□	□	□
Comments:			

.19 Does the CSO review and accept the report of the SSA when the SSA has not been carried out by the Company? (ISPS Code, paragraph B/8.13)	□	□	□
Comments:			

8.   Ship security plan (ISPS Code, sections A/9.1, A/9.4, A/9.4.1, A/9.6 and A/9.7)

	Yes	No	Other
.1 Does the CSO ensure that a ship security plan (SSP) is carried on board every ship for which he/she is the CSO? (ISPS Code, section A/9.1)	□	□	□
Comments:			

.2 Does the SSP make provisions for the three security levels as defined in this Part of the Code (ISPS Code, section A/9.1)	□	□	□
Comments:			

221

	□	□	□
.3 Does the CSO ensure that the SSP is written in the working language or languages of the ship? (ISPS Code, Part A, section 9.4)	□	□	□
Comments:			

	Yes	No	Other
.4 Is an English, French or Spanish language version also available? (ISPS Code, section A/9.4)	□	□	□
Comments:			

Part A	Yes	No	Other
.5 Does the SSP address, at least, the following: (ISPS Code, section A/9.4)			
.1 Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship?	□	□	□
.2 Identification of the restricted areas and measure for the prevention of unauthorized access to them?	□	□	□
.3 Measures for the prevention of unauthorized access to the ship?	□	□	□
.4 Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface?	□	□	□
.5 Procedures for responding to any security instructions Contracting Governments may give at security level 3?	□	□	□
.6 Procedures for evacuation in case of security threats or breaches of security?	□	□	□
.7 Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects?	□	□	□
.8 Procedures for auditing the security activities?	□	□	□
.9 Procedures for training, drills and exercises associated with the plan?	□	□	□
.10 Procedures for interfacing with port facility security activities?	□	□	□
.11 Procedures for the periodical review of the plan and for updating?	□	□	□
.12 Procedures for reporting security incidents?	□	□	□
.13 Identification of the ship security officer?	□	□	□
.14 Identification of the CSO, including 24-hour contact details?	□	□	□
.15 Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board?	□	□	□
.16 Frequency for testing or calibration of any security equipment provided on board?	□	□	□
.17 Identification of the locations where the ship security alert system activation points are provided?	□	□	□
.18 Procedures, instructions and guidance on the use of the ship security alert system including the testing, activation, deactivation and resetting and to limit false alerts?	□	□	□
Comments:			

	□	□	□

.6   Has the Company ensured that the personnel conducting internal audits of the security activities specified in the SSP, or evaluating its implementation, are independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship? (ISPS Code, section A/9.4.1)

Comments:

.7   Where the SSP is kept in electronic format, has the Company established procedures aimed at preventing the unauthorized deletion, destruction or amendment or the SSP? (ISPS Code, section A/9.6)

Comments:

.8   Has the Company established procedures to ensure the SSP is protected from unauthorized access or disclosure? (ISPS Code, section A/9.7)

Comments:

Part B – Content of SSP	**Yes**	**No**	**Other**
(ISPS Code, paragraphs B/9.1 to 9.5)			
.9 Has the CSO taken into account whether the SSP is relevant for the ship it covers? (ISPS Code, paragraph B/9.1)	□	□	□

Comments:

.10   Has the CSO complied with advice on the preparation and content of SSPs issued by the ship's Administration? (ISPS Code, paragraph B/9.1)

Comments:

.11   Has the CSO taken into account that the SSP details those items listed in ISPS Code, paragraphs B/9.2.1 to 9.2.7?

Comments:

.12   Does the CSO consider that all SSPs have been prepared having undergone a thorough assessment of all the issues relating to the security of the ship, including in particular a thorough appreciation of the physical and operational characteristics? (ISPS Code, paragraph B/9.3)

Comments:

223

	Yes	No	Other
	□	□	□

.13 Has the CSO developed the following procedures: (ISPS Code, paragraph B/9.5			
.1 To assess the continuing effectiveness of the SSP?	□	□	□
.2 To prepare amendments of the plan subsequent to its approval?	□	□	□
Comments:			

9.   Records (ISPS Code, sections A/10.1 to A/10.4)

Part A	Yes	No	Other
.1 Does the CSO ensure that records of the following activities addressed in the SSP are kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of SOLAS regulation XI-2/9.2.3: (ISPS Code, section A/10.1)			
.1 training, drills and exercises?	□	□	□
.2 security threats and security incidents?	□	□	□
.3 breaches of security?	□	□	□
.4 changes in security level?	□	□	□
.5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been?	□	□	□
.6 internal audits and reviews of security activities?	□	□	□
.7 periodic review of the ship security assessment?	□	□	□
.8 periodic review of the SSP?	□	□	□
.9 implementation of any amendments to the plan?	□	□	□
.10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system?	□	□	□
Comments:			

.2 Does the CSO ensure that the records are kept in the working language or languages of the ship? (ISPS Code, section A/10.2)	□	□	□
Comments:			

.3 Is an English, French or Spanish language version of the records also available? (ISPS Code, section A/10.2)	□	□	□
Comments:			

.4 Where the records are kept in electronic format, has the Company established procedures aimed at preventing their unauthorized deletion, destruction or	□	□	□

amendment? (ISPS Code, section A/10.3)			
Comments:			

10. Company security officer (ISPS Code, sections A/11.1 to A/11.2, A/12.2.5)

Part A	Yes	No	Other
.1 Has the Company designated one or more CSO? (ISPS Code, section A/11.1 and paragraph B/1.9)	□	□	□
Comments:			

	Yes	No	Other
.2 Where more than one CSO has been appointed, has it clearly been identified which ships each CSO is responsible for? (ISPS Code, section A/11.1)	□	□	□
Comments:			

.3 Do the CSO's duties and responsibilities include at least the following (ISPS Code, section A/11.2)			
.1 Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information?	□	□	□
.2 Ensuring that ship security assessments are carried out?	□	□	□
.3 Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan?	□	□	□
.4 Ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship?	□	□	□
.5 Arranging for internal audits and reviews of security activities?	□	□	□
.6 Arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization?	□	□	□
.7 Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with?	□	□	□
.8 Enhancing security awareness and vigilance?	□	□	□
.9 Ensuring adequate training for personnel responsible for the security of the ship?	□	□	□
.10 Ensuring effective communication and co-operation between the SSO and the relevant port security officers?	□	□	□
.11 Ensuring consistency between security requirements and safety requirements?	□	□	□
.12 Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately?	□	□	□

.4 Has the CSO implemented a mechanism for receiving from the SSO, reports of any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance, and any corrective actions taken? (ISPS Code, section A/12.2.5)	□	□	□

Comments:			

11. Training, drills and exercises on ship security (ISPS Code, sections A/13.1 to A/13.5)

.1 Have the CSO and appropriate shore-based personnel received training, taking into account the guidance given in Part B of ISPS Code? (ISPS Code, section A/13.1)	□	□	□
Comments:			

Part A	Yes	No	Other
.2 Does the CSO ensure that drills are carried out at appropriate intervals, taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, and further taking into account the guidance in Part B of ISPS Code? (ISPS Code, section A/13.4)	□	□	□
Comments:			

.3 Does the CSO ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in Part B of ISPS Code? (ISPS Code, section A/13.5)	□	□	□
Comments:			

Part B – Training, drills, and exercises on ship security (ISPS Code, paragraphs B/13.1 to B/13.4, B/13.6, B/13.7)	Yes	No	Other
.4 Have the CSO [and appropriate shore-based Company personnel] received training, in some or all of the following, as appropriate: (ISPS Code, paragraph B/13.1)			
.1 Security administrations?	□	□	□
.2 Relevant international conventions, codes and recommandations?	□	□	□
.3 Relevant Government legislation and regulations?	□	□	□
.4 Responsibilities and functions of other security organizations?	□	□	□
.5 Methodology of ship security assessment?	□	□	□
.6 Methods of ship security surveys and inspections?	□	□	□
.7 Ship and port operations and conditions?	□	□	□
.8 Ship and port facility security measures?	□	□	□
.9 Emergency preparedness and response and contingency planning?	□	□	□
.10 Instruction techniques for security training and education, including security measures and procedures?	□	□	□
.11 Handling sensitive security-related information and security-related communications?	□	□	□
.12 Knowledge of current security threats and patterns?	□	□	□
.13 Recognition and detection of weapons, dangerous substances and devices?	□	□	□

	Yes	No	Other
.14 Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security?	☐	☐	☐
.15 Techniques used to circumvent security measures?	☐	☐	☐
.16 Security equipment and systems and their operational limitations?	☐	☐	☐
.17 Methods of conducting audits, inspection, control and monitoring?	☐	☐	☐
.18 Methods of physical searches and non-intrusive inspections?	☐	☐	☐
.19 Security drills and exercises, including drills and exercises with port facilities?	☐	☐	☐
.20 Assessment of security drills and exercises?	☐	☐	☐
Comments:			

Part B	Yes	No	Other
.5 Does the CSO ensure that drills are conducted at least once every three months with additional drills as recommended in ISPS Code, paragraph B/13.6?	☐	☐	☐
Comments:			

	Yes	No	Other
.6 Does the CSO ensure that exercises are conducted at least once each calendar year with no more than 18 months between them? (ISPS Code, paragraph B/13.7)	☐	☐	☐
Comments:			

	Yes	No	Other
.7 Are these exercises: (ISPS Code, paragraph B/13.7)			
.1 Full-scale or live?	☐	☐	☐
.2 tabletop simulation or seminar?	☐	☐	☐
.3 combined with other exercises held, such as search and rescue or emergency response exercises?	☐	☐	☐
.4 participated in by the CSO?	☐	☐	☐
Comments:			

	Yes	No	Other
.8 Has the Company participated in exercises with another Contracting Government? (ISPS Code, paragraph B/13.8)	☐	☐	☐
Comments:			

12. Information and Co-operation (Best Practice)

.1 Is there a regular information exchange between the CSO and the Administration(s) responsible on best practices?	☐	☐	☐
Comments:			

Recommendations

This section should be used to record any deficiencies identified by the checklist and how these could be mitigated. In essence this will provide an action plan for the CSO and/or SSO.

Recommendations/For Action: Section 1: Continuous Synopsis Record.

Recommendations/For Action: Section 2: Ship Security Alert System.

Recommendations/For Action: Section 3: Master's discretion for ship safety and security.

Recommendations/For Action: Section 4: Obligations of the Company.

Recommendations/For Action: Section 5: Control and compliance measures.

Recommendations/For Action: Section 6: Verification and certification for ships.

Recommendations/For Action: Section 7: Ship security assessment.

Recommendations/For Action: Section 8: Ship security plan.

Recommendations/For Action: Section 9: Records.

Recommendations/For Action: Section 10: Company Security Officer.

Recommendations/For Action: Section 11: Training, drills and exercises on ship security.

Recommendations/For Action: Section 12: Information and Co-operation.

OUTCOMES

This section should be used to record the findings of the assessment and any other issues arising. These findings could be raised with ship or company personnel or be used as the basis to seek guidance from the Administration, as appropriate.

Signature of assessor	Date of completion

———————

Guidelines for Non-SOLAS Passenger Vessels

1. Preventing unauthorized access

Members of the public and passengers should not be able to gain access to operational areas of the vessel or maintenance/storage facilities such as crew rest rooms, store rooms, cleaning cupboards, hatches and lockers. All doors leading into operational areas should be kept locked or controlled to prevent unauthorized access. The only exception to this should be where access is required to reach safety equipment or to use emergency escapes. Keys for doors should be kept in a secure location and controlled by a responsible person. If access is controlled by keypad, the code should only be given to people with a legitimate need to know. It is also recommended that codes are changed periodically. Where such access controls are in place, crew should be reminded of the importance of ensuring that nobody following can bypass the access controls. The following are suggested measures to deter unauthorized access to the vessel:

- over-the-side lighting which gives an even distribution of light on the whole hull and waterline;

- keeping a good watch from the deck;

- challenging all approaching boats. If unidentified, they should, where possible, be prevented from coming alongside.

2. Conducting a search

The vessel should be searched at the start of a voyage to ensure that nothing illegal or harmful has been placed on board and at the end of a voyage to ensure that nothing has been concealed or left behind. To the extent possible, checks should include any crew areas, stores, holds, underwater hull if concern prevails and areas that could conceal persons or articles that may be used for illegal purposes. There should be agreed procedures on how to isolate a suspect package if found and how to evacuate the vessel quickly and safely. The following are examples of good practice which should be implemented to assist crew undertaking patrolling duties when operating in a higher-risk environment:

- Define the search area – crew members should be fully briefed and aware of what is required and have clearly defined start and finish points.

- Plans – laminated plans of search areas should be produced in advance, highlighting the key features of the areas to be searched (such as storage bins and emergency exits).

- Thoroughness – thorough searches help detect concealed items and attention should be paid to vulnerable areas. Crew should not rely solely on visual checks, but should take note of unusual sounds, smells, etc.

- Use of seals – un-lockable equipment boxes such as lifejacket boxes can be fitted with tamper evident seals eliminating the need to search inside unless the seal is no longer intact.

Pre-planned action – crew members should be fully briefed on their expected actions in the event a search identifies a security concern.

3. Verifying identity of persons on board a vessel

The following are examples of good practice which could be implemented to verify the identity of persons on board a vessel when operating in a higher-risk environment:

Visitors (other than passengers) should report to the Master of the vessel, or other responsible person, to notify them of their arrival and departure. All visitors should have a form of identity, for example an ID card, passport or some other form of identification bearing the individual's photograph.

Passengers must present a valid ticket before boarding (except where tickets are bought on board the vessel) and where applicable have a form of identity such as an ID card, passport or some other form of identification bearing the individual's photograph. For chartered vessels where no tickets are required, the chartering party should give some thought as to how they will control access. This could be achieved through the provision of paper authorization such as an invitation to be shown or for names on a list to be checked off on presentation of identification.

It is recommended that passengers and visitors be advised on security procedures, such as the need to:

- be escorted at all times;

- wear a permit, if issued, at all times;

- be vigilant at all times when on the vessel. Should they find a suspicious item, they should not touch it but should contact a member of crew as soon as possible. Similarly, they should contact a member of crew if they see a person acting suspiciously; and

- secure all doors behind them when leaving, particularly those doors which lead to operational areas of the vessel. If they are leaving a work site, they must ensure that it is locked and that all equipment has been securely stored.

The vessel might maintain a security log book at the point of entry/exit to the vessel, recording the identity of all persons boarding or disembarking.

4. Securing

With due regard to the need to facilitate escape in the event of an emergency, external doors and storage areas should be locked and portholes secured. If the vessel is to be left unattended for a lengthy period of time such as overnight, it is recommended that the engine is disabled to prevent theft/unauthorized use and that it is moored securely in compliance with local port by-laws. Masters should ensure that the gangway is raised when the vessel is left unattended.

5. Responding to bomb threats or discovery of suspicious items

Bomb threats are usually anonymous and communicated by telephone. While bomb threats are usually hoaxes intended to cause a nuisance, they must be taken seriously as a small number have been genuine and have preceded a terrorist or criminal act. It is recommended that advice is sought from local authorities on how to handle any genuine bomb threats that may be received.

Plans and procedures should be in place for dealing with health and safety alerts both on a vessel and at piers. These plans may be adapted to cover security alerts. Responsible individuals should consider appropriate responses for possible scenarios such as:

- Suspect packages found on board a vessel or at a pier;

- Individuals behaving suspiciously either on a vessel or at a pier;

- Security alert at another pier or on another vessel requiring suspension of operations

- A direct attack against a vessel or pier by unknown persons which could include ramming or the successful explosion of an Improvised Explosive Device.

Responsible individuals should similarly consider how to isolate a suspect package if found without removing or touching it and how to evacuate the vessel and piers quickly and safely.

If a suspicious device or package is found while a vessel is at sea, the master should take into account:

- the size and location of the device;

- the credibility of the threat;

- the vessel's location and the time it will take for security services and other assistance to arrive;

- the need to keep everyone well clear of the suspect device; and

- the need for all on board to keep clear of all doors, trunks and hatches leading from the space containing the device to avoid possible blast injuries.

6. Maintaining a means for reporting security concerns

Vessel operators should implement procedures and processes for reporting and recording security incidents. In the event of a security incident occurring while the vessel is at sea, it should be reported to the Master or SSO as appropriate. Depending on its seriousness, the Master, in addition to activating an appropriate response, may alert the nearest coastal State or authorities and/or vessels in vicinity and provide details of the incident.

Operators of non-SOLAS vessels should provide all personnel with contact information for authorities responsible for emergency response, the national response centre(s) (if appropriate) and any other authorities that may need to be notified. They should identify the actions that crew members should take in the event of a security incident

including how to notify authorities that a security incident is taking place (e.g., making radio calls, sounding alarms, etc.); and how to protect themselves, their vessel and the public.

All personnel should report suspicious activities to appropriate authorities. The report should include details of the activity and its location. The list below gives examples of activities which may by themselves constitute suspicious behaviour, any one of which may be considered suspicious by itself. However, those suspicions may warrant particular attention when one or more behaviour or a pattern of behaviour is observed or detected.

- Unknown persons photographing vessels or facilities.
- Unknown persons contacting, by any media, a ship or facility for the purpose of ascertaining security, personnel or standard operating procedures.
- Unknown persons attempting to gain information about vessels or facilities by walking up to ship or facility personnel or associated individuals, or their families, and engaging them in conversation.
- Theft or the unexplained absence of standard operating procedures documents.
- Unknown or unauthorized workmen trying to gain access to facilities to repair, replace, service, install or remove equipment.
- Inappropriate or unauthorized persons attempting to gain access to vessels or facilities.
- Theft of facility vehicles, vehicle passes, personnel identification or personnel uniforms.
- Inappropriate use of Global Maritime Distress Safety and Security procedures.
- Suspicious individuals establishing ad hoc businesses or roadside stands either adjacent to or in proximity of port facilities.
- Repeated or suspicious out of ordinary attempts at communication by voice media with duty personnel.
- Vehicles or small vessels loitering in the vicinity of a facility without due cause for extended periods of time.
- Unknown persons loitering in the vicinity of a facility without due cause for extended periods of time.

7. Prevention of trafficking in drugs and transportation of illicit cargoes

The following are general Guidelines for precautionary measures which may be taken to safeguard a non-SOLAS vessel while in port, irrespective of whether at anchor or alongside a berth, to protect the vessel against trafficking in drugs and the transportation of illicit cargoes:

- The crew should be warned about the risks of knowingly transporting illicit cargoes and trafficking in drugs.
- Crew going ashore should be advised that they should take care to ensure that persons they are meeting with are not connected with illegal activities.
- The vessel might maintain a security log book at the point of entry/exit to the vessel, recording the identity of all persons boarding or disembarking. No unauthorized persons should be allowed to board.
- A permanent watch may be advisable in working areas. If appropriate, areas such as the forecastle, poop deck, main decks, etc., must be well lit during the hours of darkness.
- The vessel should maintain a good lookout for approaching small boats, or the presence of unauthorized divers, or other attempts by unauthorized persons to board the vessel.
- In the event of drugs or illicit cargoes are found on board, the crew should cooperate fully with the local authorities for the duration of the investigation.

8. Prevention of stowaways

For the purposes of the Guidelines a stowaway is defined as a person who is secreted on a vessel, or in cargo which is subsequently loaded onto a vessel, without the consent of the vessel owner or the master or other responsible person, and who is detected on board after the vessel has departed from a port and is reported as a stowaway by the master to the appropriate authorities.

The visible actions of the crew in implementing security measures will act as a deterrent to potential stowaways. Examples of general precautionary measures for the prevention of stowaways are set out below:

- Prior to entering port, doors and hatchways should be securely fastened and locked with due regard to the need to facilitate escape in the event of an emergency.

- Fitting plates over anchor hawse pipes can prevent stowaways from boarding at anchorage or before a vessel is berthed.

- Accommodation doors could also be secured and locked, leaving only one open entrance. In the interests of safety, keys to the locked doors should be placed in convenient positions so that doors can be opened in the event of emergency.

- Store rooms, equipment lockers on deck, the engine room and the accommodations should remain locked throughout a port call, only being opened for access and re-secured immediately thereafter.

- Once alongside, a gangway watch is the first line of defence against stowaways, smugglers and theft. For this reason, it is important to ensure that an effective gangway watch is maintained at all times.

- At the commencement of loading only the hold access doors of the compartments that are going to be used for the immediate loading of cargo should be opened. As soon as cargo operations cease, the compartment should be secured.

- The vessel's storerooms should also be kept locked at all times, only being opened when access is required.

- There may be some areas of the vessel that cannot be locked, for instance the funnel top. Any unlocked areas that can be accessed should be inspected on a regular basis.

- On completion of cargo loading operations and the disembarkation of all shore-based personnel, accessible areas of the vessel should be searched again.

- In high-risk ports consideration should be given to anchoring in some convenient position outside the port and making a final stowaway search after tugs and pilots depart.

- If possible, the search should be conducted by two crew members. In the event that a stowaway is found, this will reduce the risk of the stowaway attacking or overpowering the searcher

A detected stowaway should be reported immediately to the appropriate authorities. Any stowaways detected should be treated in accordance with humanitarian principles. However, as some stowaways may be violent, direct engagement is discouraged as the safety and security of the vessel and its crew should not be compromised.

Specific Guidelines for Non-SOLAS Passenger Vessels

These guidelines are intended to complement the general guidelines contained above.

1. Searching

It is recommended that passengers are not permitted to board until the security check of the vessel has been completed. To the extent possible, checks should include all public areas with special attention paid to underneath seating, toilets, and any storage areas, e.g., for luggage, on the vessel.

2. Control of passengers boarding and disembarking

Passengers must only be allowed to embark and disembark if crew or shore staff are present. Where ticket facilities exist for scheduled services, crew or shore staff should ensure that passengers present valid tickets before boarding. For chartered vessels where no tickets are required, the chartering party should seek to control access on to the boat, for example through the provision of an authorization card. If the vessel carries vehicles special additional measures, including spot checks, may be required.

3. Passenger security awareness

Passengers should be reminded not to leave bags unattended and to report any unattended or suspect packages. Security messages should be displayed on posters and information screens and should be frequently delivered over public address systems either as separate announcements or as part of the pre-sailing safety announcement.

Specific Guidelines for Pleasure Craft

1. Introduction

Each national authority has its own definition of Pleasure Craft and may apply these guidelines as appropriate Although they focus on pleasure craft engaged in international voyages or operating in waters where they might interact with or operate in close proximity to ISPS Code-compliant vessels or port facilities, they may have broader implementation as many pleasure craft are highly mobile, both via land and connecting waterways. The Guidelines are intended to complement the general guidance contained in Appendix F2.

Pleasure craft owners and operators should remember that the overall safety and security of the vessel, crew, and passengers is their responsibility. Prudent mariners are proactive in preventing incidents, planning in advance how best to respond to an incident, ensuring that all passengers and crew members know their roles; and being familiar with any particular directions that exist for an intended port or destination. Owners and operators should consider designating one crew member as responsible for all aspects of the security on the vessel. Some companies now offer courses specifically tailored for blue-water yachtsmen.

2. Security measures for unattended pleasure craft

Possible measures include:

- Locking ignition switches and steering.
- Fitting a small craft alarm system, possibly with an autodial facility to alert an operator to any unauthorized movement, or the activation of a variety of on board security sensors, via Cell Phone or e-mail. The alarm system could also be integrated with smoke and fire sensors for a complete vessel protection system.
- Securing high value items so that they are out of sight and in lockable compartments.
- Not leaving anything valuable on display and preferably removing them e.g. the ignition key.
- Marking equipment using approved property marking equipment.
- Etching the hull identification number onto windows and hatches.
- Installing an engine immobilizer or a hidden device to shut off the fuel line.
- Securing outboard motors with a strong case-hardened steel chain padlock, chain or some form of proprietary locking bar.
- Covering the boat as far as the design allows and securing the cover.
- Photographing the vessel and equipment (to assist authorities in returning stolen equipment)
- Recording all available serial numbers and storing them in a safe place on and off the vessel.
- Acquiring Radio Frequency Identification Tag (RFID) anti-theft systems (not only do such systems have the potential to reduce theft risk, but they also have been shown to increase recovery rates and in some instances to reduce insurance fees).

3. Higher risk environments

Where safe and secure routes are not practicable, transits should be accomplished in the presence of other vessels, as expeditiously as possible, and prior notification made to the maritime authorities for the area whose advice should be followed. A rigorous contact schedule should be maintained, preferably via satellite or mobile telephone or similar system which cannot be used to locate the vessel via radio direction finding.

Consideration should be given to providing operator proficiency training for pleasure craft owners and operators that encompasses security awareness familiarization.

4. Arrival and Departure Information

Pleasure craft departing a port could be required to submit voyage information when applying for port clearance, as has been implemented by Singapore. The voyage information may include the estimated time of departure, destination and the planned route of the trip. The additional information may be useful to the relevant authorities not only in monitoring and enforcement activities, but also when conducting search and rescue operations should the vessel run into trouble and require assistance. For more information refer to: *Declaration of Information by Pleasure*

234

Craft Departing Singapore, Singapore, Maritime and Port Authority, Port Marine Circular No.17, 25 April 2003 , at the following website: www.mpa.gov.sg/sites/circulars_and_notices/pdfs/port_marine_circulars/pc03-17.pdf

5. Registration

Some national authorities are encouraging operators of pleasure craft to register with their Maritime Administration or delegated organization which could provide a database available for authorized online access to assist in both preventative and response activities related to both safety and security. One such example is the UK Ship Register, Part 3, Pleasure Craft/Small Ships, at the following website: www.mgca.gov.uk .

The registry is cheaper and simpler than full vessel registration and specifically aimed at pleasure craft. Owners benefit by having details of their craft's nationality and registered keeper recorded by an authoritative organization. It can be applied for on-line. However, it should be noted that registration in itself offers no protection against the misuse of a registered pleasure craft which may be stolen, hijacked or even legally acquired.

6. Information Sharing

Some national authorities are seeking agreements to provide for information sharing, within the context of their individual laws and regulations, possibly as part of their individual coastal security initiatives. Pleasure craft engaged in international voyages present unique circumstances. Even when registered, information regarding vessel characteristics, ownership, etc., is often not shared between countries of departure and arrival. This can result in a lack of transparency for security and safety organizations, leading to, for example, complications in validating an arriving vessels identity.

7. Ship Security Plan

Some national authorities have issued guidelines on developing effective security measures to address threats and other incidents at sea. One such authority is the International Merchant Marine Registry of Belize (IMMARBE) which has issued *Guidelines for an effective Ship Security Plan for yachts not required to hold ISPS Code certification.* They may be accessed at the following website: www.immarbe.com/yachts/guide_ship_security.html

Section 5 Framework for Conducting Security Assessments

5.1　Introduction

5.1.1　As noted in paragraphs 2.8.25 to 2.8.33 and 2.9.12 to 2.9.14, security assessments provide the foundation for the effective implementation of the Maritime Security Measures at port facilities and on-board ships.

5.1.2　In December 2008, the IMO issued guidance to assist national authorities in undertaking risk assessments. Although this guidance was aimed at non-SOLAS vessels, the methodology and the principles on which it is based are equally applicable to SOLAS port facilities and ships.

5.1.3　Although there are many different techniques which range in the complexity of their application, the following six phases are common to all:

    a   Pre-Assessment
    b   Threat Assessment
    c   Impact Assessment
    d   Vulnerability Assessment
    e   Risk Scoring
    f   Risk Management

5.1.4　Each of the phases is discussed in turn below.

5.2　Pre-Assessment Phase

5.2.1　Effective project management is essential to the successful conduct of a security assessment. Before starting an assessment, the following steps should be considered.

Risk Register

5.2.2　A useful first step is to establish a risk register that summarizes the assessment and scoring phases identified above. A sample format is shown below, along with accompanying explanations.

Reference number – each threat scenario (TS) should be assigned a reference number so that it can be easily identified and its development tracked	Threat scenario – each possible threat scenario shouuld be named with a brief description of what it entails.	Lead organization – refer to sub-section 5.3	Support organizations – refer to sub-section 5.3	Threat (likelihood) – refer to sub-section 5.3	Impact – refer to sub-section 5.4	Vulnerability			Risk score- refer to sub-section 5.6
						Key assets – refer to sub-section 5.5	Mitigating controls – refer to sub-section 5.5	Vulnerability score – refer to sub-section 5.5	
TS 1									
TS 2									

Establishing Assessment Teams

5.2.3   As the Maritime Security Measures identify both the conduct and approval of a PFSA to be a responsibility of the Designated Authority, the team leader should be a government official appointed by the Designated Authority. However, as the conduct of a PFSA requires extensive input from the port facility, representatives of the facility operator including the PFSO should be team members.

5.2.4   Although the Maritime Security Measures do not require government officials to be involved in the conduct or approval of a SSA, a small assessment team could still be established. Normally, its leader would either be the CSO or a suitably qualified member of the RSO to which the assessment has been delegated.

5.2.5   Where possible, assessment teams should follow project management principles in planning and conducting an assessment.

5.2.6   Experience to date indicates that the assessment team should ensure that the operator is well-briefed on how the assessment is to be conducted. This is often achieved through the provision of an information package with follow-up as required by the team leader.

Process Mapping

5.2.7   Where possible, the assessment process should be mapped as a basis for identifying critical path items and responsibilities. The flow chart below provides an example of the main steps in a typical assessment.
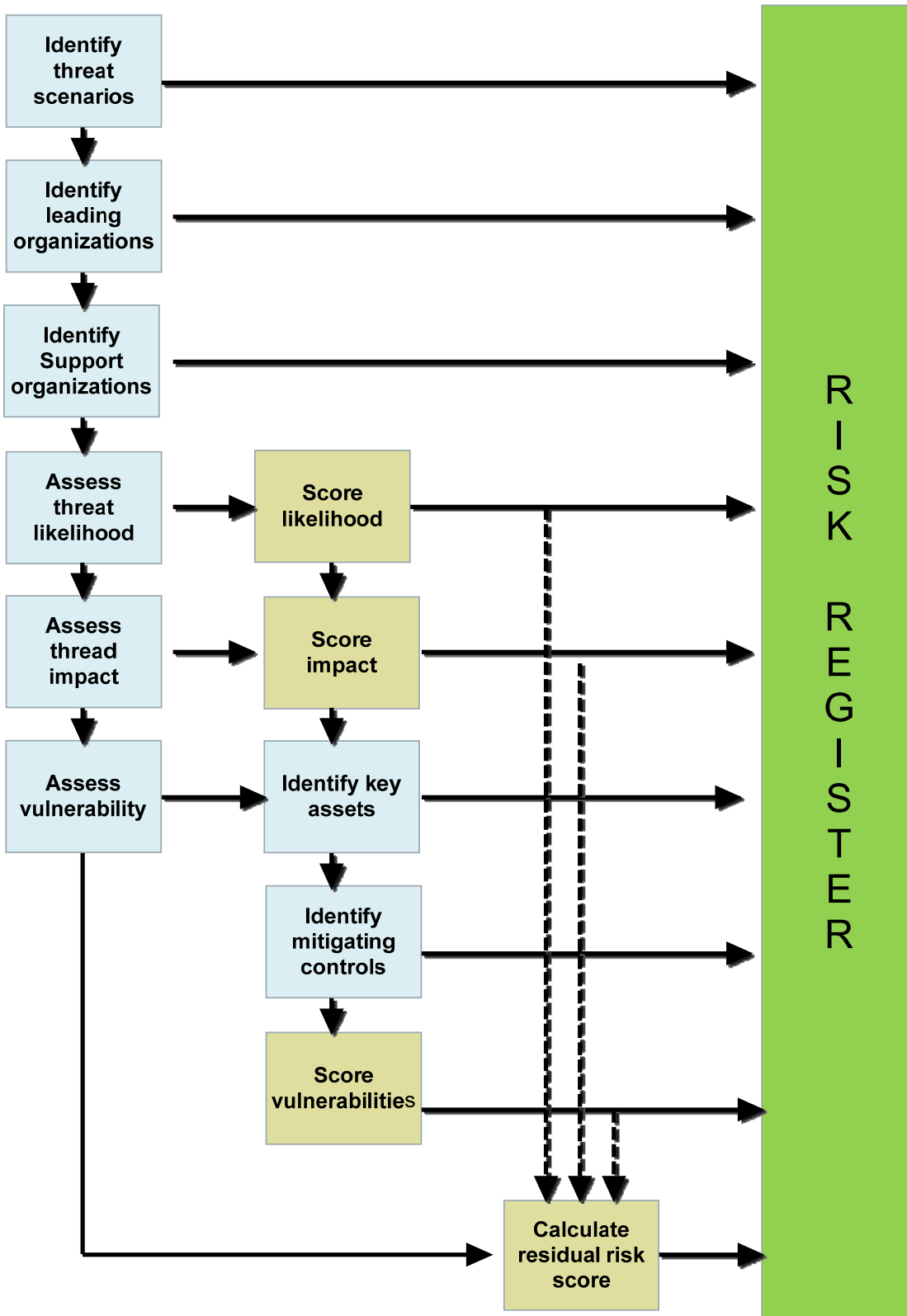
Risk assessment flowchart

Inventory Development

5.2.8   An inventory should be prepared of:
   a   Assets and infrastructure;
   b   Operating procedures;
   c   Site or ship layout plans;
   d   Previous security assessments;
   e   Current security plan;
   f   Previously reported security incidents;
   g   Control measures in place; and
   h   Risk-based classification based on type of facility or ship.

Methodology Selection

5.2.9   The final pre-assessment task is to select the appropriate methodology. This is based in large part on the risk-based classification of the type of port, port facility or ship. The methodology used for a small, single purpose port facility or small general cargo ship is likely to be less complex than the methodology required for a large, multi-purpose facility or cruise ship.   The methodology described below should be suitable for most port facilities, small to medium-sized ports and most ships.

5.2.10   Internet sources of security assessment methodologies are shown in Appendix 5.1 – Examples of Internet Sources of Security Assessment Methodologies.

5.3   Threat Assessment Phase

5.3.1   The first step is to list and agree on which threat scenarios could apply. Useful tips include:
   a   Preparing an initial list of threat scenarios;
   b   Having a "brainstorming" session where subject matter experts consider if there are any additional scenarios which should be listed and any refinements needed to develop to the initial list;
   c   Identifying potential perpetrators (e.g. terrorists, criminals, activists, disruptive passengers, employees);
   d   Considering how they might operate (e.g. by reference to any precedents);
   e   Considering their possible motivation and intent (e.g. financial gain, publicity, vengeance); and
   f   Considering their capability to act (e.g. numbers, training, funding, weapons, track record, support).

5.3.2   The next step is to identify the lead organization or coordinating body identified so that initial points of contact and responsibilities may be established for each scenario. Lead organizations should meet one of the following criteria:
   a   own the assets;
   b   set the policy for dealing with the threat;
   c   have legal responsibility for, or have the major role in, mitigating or responding to a particular threat; or
   d   a combination of the above.

5.3.3   As there may be a different lead organization in instances where responsibilities vary depending on type of threat, location and method, distinctions should be made where appropriate between responsibilities for:
   a   preventive/protective security measures;
   b   contingency planning and reactive security measures to deal with and contain an incident;
   c   implementing the above measures.

5.3.4   Support organizations (e.g. first responders) should also be identified as they have a role in mitigating the threat but do not meet the criteria listed above for lead organizations. It may be decided that all stakeholders are support organizations through being vigilant, providing a deterring presence and sharing information with others.

5.3.5   For some threat scenarios, identifying lead and support organizations is not a simple task. If there are differing views, it is important that consensus is reached, particularly as lead organizations have a primary role in developing and delivering action plans. In situations where more than one lead organization is identified, it may be worth re-evaluating to minimize the potential for confusion and duplication.

5.3.6   The final step in this phase is to assign a score to each threat scenario. The score should reflect the likelihood of each threat scenario occurring if there were no security measures or mitigating controls in place to prevent them. To accurately score the threat, assessors should:

a   consider local and international intelligence/knowledge about similar events which have or could have occurred;

b   discuss how likely it would be for each threat scenario to occur if there were no security measures in place;

c   read the definitions in the table below and decide which score best applies.

d   use an alternative method of scoring if it produces a more logical and accurate assessment of the threats and risks;

e   remember to apply any agreed rules around confidentiality.

Score	Likelihood	Criteria
4	PROBABLE	There have been previous reported incidents. There is intelligence to suggest that there are groups or individuals capable of causing the undesired event. There is specific intelligence to suggest that the port, port facility, ship or type of ship is a target.
3	LIKELY	There have been previous reported incidents. There is intelligence to suggest that there are groups or individuals currently capable of causing the undesired event. There is general intelligence to suggest that the port, port facility, ship or type of ship may be a likely target.
2	UNLIKELY	There is intelligence to suggest that there are groups or individuals capable of causing the undesired event. There is nothing to suggest that the port, port facility, ship or type of ship is a target.
1	IMPROBABLE	There have been no previously reported incidents anywhere worldwide. There is no intelligence to suggest that there are groups or individuals capable of causing the undesired event.

5.4   Impact Assessment Phase

5.4.1   The first step is to list examples of the type and magnitude of impact that might be expected if an undesired event happened. As the list of undesired events and their impacts in the table below are not exhaustive, assessors should consider modifying the table to meet their needs and to record discussions on the type and magnitude of impact associated with each listed undesired event.

Type of undesired event	Loss of life or personal injury	Loss or damage to ship & ship infrastructure	Loss of use of equipment	Disruption to services	Financial loss to vessel	Damage to reputation	Publicity to perpetrator
Explosive Device (IED)							
Sabotage							
Arson							
Unauthorized access							
Theft of vessels							

5.4.2 The second step is to assign a score to each impact. To score the impact accurately, assessors should:

a read the definitions in the table below and decide which one best applies to each undesired event in terms of its impact on the port facility or ship if the event occurs but without mitigating factors in place.

b consider how to record the scores allocated under each of the column headings for each undesired event. For simplicity, an average may be taken in most cases of the scores assigned to applicable impacts. If a particular impact is not applicable, it should be noted as such and excluded from the averaging process.

Score	Impact	Criteria – Potential for:
4	SUBSTANTIAL	Multiple fatalities. Serious loss or damage to assets, infrastructure or ship. Economic cost of more than an agreed-on amount. Widespread coverage resulting in serious damage to reputation.
3	SIGNIFICANT	Loss of life. Significant but repairable loss or damage to assets, infrastructure or craft. Economic cost of less than an agreed-on amount. National adverse media coverage.
2	MODERATE	Major injuries. Short-term minor loss or damage. Economic cost of less than an agreed-on amount. Major local damage to reputation.
1	MINOR	Minor injuries. Minimal operational disruption. Economic cost of less than agreed-on amount. Minor damage to reputation.

5.5 Vulnerability Assessment Phase

5.5.1 The first step involves listing:

a the most important assets or targets including infrastructure which could be affected by the scenario e.g. people (crew and passengers), objects, physical infrastructure and equipment; and

b their relevant characteristics and how they can be exploited.

5.5.2 Experience to date indicates that this is often achieved through an on-site or on-board survey by the assessment team.

5.5.3 The next step involves identifying the current mitigating controls (i.e. the security measures which are already in place to protect the key assets) and assessing their effectiveness and residual weaknesses. This is a vital step but, depending on the technique used, can be time-consuming, complex and intensive. As a minimum, assessors should undertake on-board or on-site inspections as a way of enhancing their understanding of the key assets or targets and the effectiveness of the mitigating controls in place. More sophisticated techniques (e.g. process mapping and event cause analysis) may provide for a more thorough assessment but should only be undertaken by individuals trained in their application.

5.5.4 Assessors may want to create a table similar to the one below to record their preliminary findings. This is a useful review tool to reconsider the effectiveness of control measures highlighted in the risk register and identify where there are weaknesses and gaps. Knowledge of those assets judged to be of high importance helps risk assessors to focus their review on what safeguards are in place and hence assess the vulnerability more accurately.

Assessment of security measures used to counter breaches of security

Security Measures	Intended Results
Security patrols	Deterrence and detection
Monitoring of security equipment	Pre-empt breach or swift response
Education and training of employees	Employee awareness
Possible Weaknesses	**Follow-up Actions**
Inadequate resources	Discuss issues with relevant personnel
Gaps in security coverage	Consider redeployment of resources
Insufficient training	Organize employee training programme

5.5.5   Assessors may also find it useful to ask the following questions and complete the table below, as they proceed through this phase:

   a   What are the key targets – people, critical infrastructure, communications and control, and support services?

   b   What are the systems designed to deter, detect, delay or deal with unlawful acts?

   c   What are the weaknesses in these systems, including consideration of predictability and opportunity?

   d   Which assets are high value?

   e   Which stakeholders have a part to play in reducing the vulnerability of the target?

   f   How will this assist in defining "who" should work together on what?

	KA1	KA2
Target – list of key assets (KA) grouped by category (e.g. infrastructure, communications and control assets, support services, people).		
Strengths – systems designed to deter, detect, or deal with undesired events (e.g. vetting/pass systems, CCTV, restricted areas and police presence).		
Weaknesses – includes limited intelligence indicating the likelihood of a threat and the desirability of the target for the perpetrator (e.g. due to lack of search capability, poor surveillance, high traffic volumes, personnel shortages).		
Opportunities – opportunities for the perpetrator to exploit a loophole, conduct reconnaissance, etc.		
Predictability – the ways in which a target operates which make it predictable.		
Vulnerability – a High-Medium-Low rating based on a preliminary assessment of the net effect of the vulnerability factors identified above.		
Stakeholders involved in reducing vulnerability - includes members of port and ship security committees.		
Means of reducing vulnerability.		

5.5.6   The final step of this phase involves translating the vulnerability assessment into a vulnerability score. It requires consideration of, on the one hand, an evaluation of targets' characteristics and, on the other, the early warning indicators, embedded monitors and existing mitigating controls. The table below illustrates a possible scoring system to be used for assessing vulnerability using the example of access to sensitive area outside the boundary of a restricted area.

Score	Extent of risk management	Counter measures in place
4	None	None
3	Limited	Some
2	Acceptable	Sufficient to manage the threat down to an acceptable level
1	Robust and effective	Complete set

5.6   Risk Scoring Phase

5.6.1   All the information gathered on threat, impact and vulnerability should be used to identify and assess the residual risk. To score the risk accurately, assessors should use the formula:

RISK = THREAT x IMPACT x VULNERABILITY

5.6.2   For example, using an initial threat score of 2, an impact score of 4 and, where there are no mitigating measures in place (a vulnerability score of 4), the residual risk score would be 32 (2 x 4 x 4). Where measures are judged to reduce the vulnerability to some extent, but not to an acceptable level, the residual score would be 24. The threat and impact scores of 2 and 4 remain but the vulnerability score is now 3; hence 2 x 4 x 3 = 24. And so on. As there is a presumption that no threat scenario can be managed totally out of existence, a score of 0 is not possible.

5.6.3   It should be noted that scenarios with differing individual threat, impact and vulnerability scores can have the same overall risk score. For instance a particular scenario may have a threat score of 4 an impact score of 2 and a vulnerability score of 2 whereas another scenario may have a threat score of 1, an impact score of 4 and a vulnerability score of 4. Both scenarios produce a risk score of 16 despite having differing individual values of threat, impact and vulnerability.

5.6.4   Experience to date indicates that risk can be ranked into three broad categories - high, medium and low – as illustrated below:

    a   HIGH - a residual risk score of 27 or more.

    b   MEDIUM - a residual risk score of between 8 and 24.

    c   LOW - a residual risk score of 6 or less.

5.7   Risk Management Phase

5.7.1   This phase considers how best to address the weaknesses identified during the vulnerability and risk scoring stages and how to mitigate the risk effectively and practically on a sustainable long-term basis. This can be achieved by all stakeholders working together to agree joint tactical action plans' an example of which is shown below.   The checklist below gives some pointers on how to work through the process:

    a   Consider the overall risk profile from the risk register:
- High = Unacceptable Risk – seek alternative and/or additional control measures,
- Medium = Manageable risk – requires management/monitoring,
- Low = Tolerable risk – no further control measures needed.

    b   Reconsider the Security Measures Review table in paragraph 5.5.4 above; the "possible weaknesses" and "follow-up actions" should assist in drawing up action plans.

    c   Agree the priorities for action; these should be the "high" risks in the first instance.

    d   Identify what actions can and need to be taken to bring the risk down to a "medium" (manageable risk) and from there to a "low" (tolerable risk).

    e   Agree on the lead agency in implementing changes.

    f   Consider the resource implications.

    g   Document recommendations, actions taken and link these back to the threats in the risk register.

    h   Agreed actions should be recorded and progress monitored; such records are also evidence of decisions taken.

    i   Determine the approval level for the action plan recommendations.

    j   Consider the need to develop further systems for sharing information and intelligence.

    k   Look for opportunities to share resources and assist others.

    l   Establish a re-assessment schedule (e.g. as conditions change or on a regular schedule).

5.7.2   A sample action plan is illustrated on the following page.

Sample Action Plan

Ref Number:	
THREAT:	
Current Risk status:	
Area of port:	
Lead Agency:	

Current Controls:

Weaknesses:

Review of residual risk:

Date of review:	

AGREED ACTIONS: **CURRENT STATUS**

		GREEN

Timescale for review:

CURRENT STATUS KEY

RED	Behind schedule, no remedial action in place
AMBER	Falling behind schedule, remedial action in place
GREEN	On track

1. Threat and Risk Analysis Matrix (TRAM)

Source: ILO/IMO Code of Practice on Security in Ports

Purpose: To provide smaller ports with few significant facilities and ports located in isolated areas with a practical risk assessment and management tool.

Summary Description: TRAM is a simplified version of the tool described above. It is a 10-step methodology which produces a risk score for each identified threat scenario as a basis for assigning priorities to security measures identified in an action plan. The tool is demonstrated by an example based on a specific threat scenario – destruction of a port authority's communication tower by explosives.

Internet Site: www.imo.org

2. Port Security Risk Assessment Tool (PSRAT)

Source: United States Coast Guard (USCG), International Port Security Program

Purpose: To provide U.S. Coast Guard Captains of the Port with a methodology for performing a risk-based analysis of assets and infrastructure within their area of responsibility.

Summary Description: PSRAT is a more sophisticated version of the TRAM tool described above. It is a multi-step automated tool created as a Microsoft Access 2000-based application. Input screens are used to capture the data needed for the analysis; all data are stored in the Access database. Unlike manual techniques, PSRAT facilitates the ability to update risk scenarios and their associated risks, identify the key drivers of risk scores and estimate the effectiveness of countermeasures.

Internet Site: www.homeport.uscg.mil PSRAT has been placed on the Best Practices website to enable its use as a template by other government entities for their own risk assessment purposes. The site contains two supporting documents including the PSRAT User's Manual.