INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1525
1 June 2016

GUIDANCE FOR THE DEVELOPMENT OF NATIONAL MARITIME SECURITY LEGISLATION

1 The Maritime Safety Committee, at its ninety-sixth session (11 to 20 May 2016), having considered the need to assist Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, as amended (the Convention), with the development of national legislation related to the implementation of the provisions of chapter XI-2 of the Convention and the International Ship and Port Facility Security (ISPS) Code, approved the *Guidance for the development of national maritime security legislation*, as set out in the annex.

2 This Guidance is drawn from the Convention, parts A and B of the ISPS Code, the 2012 "Guide to Maritime Security and the ISPS Code", as well as related IMO resolutions and circulars.

3 While this Guidance refers to mandatory provisions from the Convention, as well as both mandatory provisions and guidance in the ISPS Code, the use of this Guidance is not mandatory.

4 Contracting Governments to the Convention willing to use this Guidance for the development of their own maritime security legislation may request technical assistance by contacting the Secretariat at marsec@imo.org.

***

ANNEX

GUIDANCE FOR THE DEVELOPMENT OF NATIONAL MARITIME SECURITY LEGISLATION

3.2 Ship Security Officer
3.2.1 Ship Security Officer – General
3.2.2 Ship Security Officer – Qualifications
3.2.3 Ship Security Officer – Duties
3.3 Shipboard personnel
3.3.1 Shipboard personnel – Qualifications
3.4 Documentation
3.4.1 Ship security assessment
3.4.2 Ship security plan
3.5 Training, drills and exercises
3.5.1 Training
3.5.2 Drills
3.5.3 Exercises
3.6 Physical security
3.6.1 Restricted areas
3.6.2 Access points
3.6.3 Signage
3.6.4 Identification
3.6.5 Lighting
3.6.6 Surveillance
3.6.7 Communications
3.7 Operational security
3.7.1 Master's discretion
3.7.2 Port control compliance
3.7.3 Manning requirements
3.7.4 Access control
3.7.5 Cargo operations
3.7.6 Ship's stores
3.7.7 Unaccompanied baggage procedures
3.8 Security obligations
3.8.1 International Ship Security Certificate (ISSC)
3.8.2 Communications/reporting procedures
3.9 Incident response
3.9.1 Security incidents
3.9.2 Unauthorized access/breach procedures
3.9.3 Best management practices

Part 4 – Port facility security
4.1 Port Facility Security Officer
4.1.1 Port Facility Security Officer – General
4.1.2 Port Facility Security Officer – Qualifications
4.1.3 Port Facility Security Officer – Duties
4.2 Port Security Committee
4.2.1 Port Security Committee – general
4.3 Documentation
4.3.1 Port facility security assessment
4.3.2 Port facility security plan
4.3.3 Statement of compliance
4.4 Training, drills and exercises
4.4.1 Basic port security knowledge
4.4.2 Training
4.4.3 Drills
4.4.4 Exercises
4.5 Physical security

Preamble

Although the International Ship and Port Facility Security (ISPS) Code came into effect on 1 July 2004, gaps in its implementation and application still persist. Many Governments[1] are still striving to implement fully the maritime security measures, particularly those pertaining to port facilities, due to a variety of factors, including the lack of legal and policy instruments required to achieve compliance with the ISPS Code and to resolve jurisdictional issues between Government agencies.

Essential to the successful implementation and oversight of the ISPS Code is the drafting and enactment of appropriate national legislation to provide for the full implementation and oversight of the maritime security measures. The legislation should 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.

Most Governments have enacted legislation to implement the ISPS Code. 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. National legislation has generally focused on the mandatory requirements in part A of the ISPS Code, but 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 of the ISPS Code mandatory.

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.

To implement fully the requirements in the maritime security measures, the legislation should cover:

.1 definitions;

.2 application;

.3 Designated Authority and Administration;

.4 security levels;

.5 port facilities;

.6 Port facility security assessments;

.7 ship;

.8 Port facility security plans and ship security plans;

.9 retention of records and declarations of security;

[1] The term "Governments", when used in this Guidance, refers to Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, as amended.

.10 inspection of port facilities and ships;

.11 enforcement action;

.12 control and compliance measures; and

.13 offences relating to the maritime security measures.

This Guidance is drawn exclusively from IMO sources. In addition to the International Convention for the Safety of Life at Sea, 1974, as amended (SOLAS) and Parts A and B of the ISPS Code, it includes as well relevant extracts from the 2012 Guide to Maritime Security and the ISPS Code (GMSIC) and a variety of IMO resolutions and circulars. A full list of source documentation is provided in the appendix. While this compilation provides the framework to assist in the development of national legislation, it is not intended as an auditing or assessment tool.

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 this guidance to the consistent use of verbs as follows: mandatory text uses "must" or "shall", as appropriate; and guidance text uses "may" or "should", as appropriate. Furthermore, optional guidance text, which relates to non-mandatory provisions, has been italicized to further clarify the distinction.

Part 1 – General provisions

1.1 Short title and commencement

1.1.1 This [_____] establishes a framework of measures to enhance maritime security and through which ships and port facilities can cooperate to detect and deter acts which threaten security in the maritime transport sector.

(ISPS Code, part B, paragraph 1.1)

1.2 Purpose

1.2.1 The purpose of this [_____] is to promulgate all laws, decrees, orders and regulations necessary to give full and complete effect to chapter XI-2 of the Convention for the Safety of Life at Sea, 1974, as amended (SOLAS), and the International Ship and Port Facility Security (ISPS) Code.

(SOLAS, art. I(b)).

1.3 Application

1.3.1 This [_____] applies to:

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

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

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

.2 mobile offshore drilling units; and

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

(SOLAS regulation XI-2/2.1)
(ISPS Code, part A, paragraph 3.1)

1.4 Definitions

1.4.1 The definitions used in this [_____] should, as far as appropriate, be similar to those used in the ISPS Code.

(GMSIC, paragraph 2.2.18)

Part 2 – National authorities for ship and port facility security

2.1 National authorities – General

2.1.1 The government should specify which organization within the 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 may be combined in a single organization.

(GMSIC, paragraph 2.2.22)

2.2 National authorities – Duties

2.2.1 Pursuant to SOLAS chapter XI-2 and part A of the ISPS Code, [the specified organization(s)] is/are responsible for:

.1 setting the applicable security level;

.2 approving the Ship security plan and relevant amendments to a previously approved plan;

.3 verifying the compliance of ships with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code and issuing to ships the International Ship Security Certificate;

.4 determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port facility security plan;

.5 ensuring completion and approval of the Port facility security assessment and of any subsequent amendments to a previously approved assessment;

.6 approving the Port facility security plan and any subsequent amendments to a previously approved plan;

.7 exercising control and compliance measures;

.8 testing approved plans; and

.9 communicating information to the International Maritime Organization and to the shipping and port industries.

(ISPS Code, part B, paragraph 1.6)

2.3 National authorities – Powers

2.3.1 National authorities – Security level/governance authority

2.3.1.1 [The specified organization] shall set security levels and ensure the provision of security-level information to ships entitled to fly the flag of [State].

2.3.1.2 [The specified organization] shall set security levels and ensure the provision of security-level information to port facilities within [State].

2.3.1.3 Factors to be considered in setting the appropriate security level include:

.1 the degree that the threat information is credible;

.2 the degree that the threat information is corroborated;

.3 the degree that the threat information is specific or imminent; and

.4 the potential consequences of such a security incident.

(SOLAS regulation XI-2/3)
(ISPS Code, part A, paragraph 4.1)

2.3.2 National authorities – Regulatory authority

2.3.2.1 [The specified organization] shall promulgate regulations and take all other steps necessary to give full and complete effect to the security directives of the Administration and designated authority in accordance with [State] constitution and laws.

(SOLAS, art. I(b))

2.3.3 National authorities – Inspection authority

2.3.3.1 Officers undertaking inspections for [the specified organization] 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 may include:

.1 access control, including to restricted areas;

.2 handling of cargo;

.3 delivery of ship's stores and bunkers;

.4 monitoring the port facility;

.5 handling threats, breaches of security and security incidents;

.6 security communications;

.7 audits and amendments;

.8 procedures for shore leave and visitors to the ship;

.9 procedures for ship-to-shore interface activities;

.10 evacuation procedures; and

.11 protection of sensitive security information, e.g. the security plan.

(GMSIC, paragraph 2.17.13)

2.3.4 National authorities – Enforcement authority

2.3.4.1 [State] legislation should specify the powers needed for Government officials to undertake the application of enforcement actions to correct incidents of non-compliance.

(GMSIC, paragraph 2.2.3)

2.3.5 National authorities – Delegation authority

2.3.5.1 [The specified organization] may delegate power to act on their own behalf, in the organization's name.

(GMSIC, paragraph 2.2.23)

2.3.6 Alternative security agreements

2.3.6.1 Governments may conclude in writing bilateral or multilateral agreements with other Governments on alternative security arrangements covering short international voyages on fixed routes between port facilities located within their territories.

(SOLAS regulation XI-2/11.1)

2.3.7 Equivalent security arrangements

2.3.7.1 [The specified organization] may allow a particular ship or a group of ships entitled to fly its flag, or a port facility or a group of port facilities located within the Government's territory to implement other security measures equivalent to those prescribed in SOLAS chapter XI-2 or in part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in SOLAS chapter XI-2 or in part A of the ISPS Code.

(SOLAS regulation XI-2/12)

2.4 National Maritime Security Committee

2.4.1 National Maritime Security Committee – General

2.4.1.1 A national maritime security committee should be formed to address the development, relevance and acceptability of a national maritime security framework or strategy.

(GMSIC, paragraph 2.4.9)

2.4.2 National Maritime Security Committee – Qualifications

2.4.2.1 A national maritime security committee should involve representatives of those regulated: major stakeholders in the port and shipping industries, port workers and seafarers, and cargo and passenger interests.

(GMSIC, paragraph 2.4.9)

2.4.3 National Maritime Security Committee – Duties

2.4.3.1 The national maritime security committee should:

.1 identify security threats and vulnerabilities;

.2 establish security priorities;

.3 plan, coordinate and evaluate security initiatives;

.4 develop or contribute to a national maritime security framework or strategy;

.5 develop or contribute to Government policy statements on maritime security;

.6 develop coordinated positions on meeting international obligations;

.7 address jurisdictional issues involving member organizations; and

.8 handle major security issues, with multi-organization implications, referred to the committee by high-level committees.

(GMSIC, paragraph 2.4.16)

2.5 Recognized security organizations

2.5.1 Recognized security organizations – General

2.5.1.1 Governments may delegate to a recognized security organization certain of their security-related duties under SOLAS chapter XI-2 and part A of the ISPS Code.

(ISPS Code, part A, paragraph 4.3)

2.5.2 Recognized security organizations – Qualifications

2.5.2.1 When authorizing a recognized security organization, [the specified organization] should give consideration to the competency of such an organization. A recognized security organization should be able to demonstrate:

.1 expertise in relevant aspects of security;

.2 appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;

.3 capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimize such risks;

.4 ability to maintain and improve the expertise of their personnel;

.5 ability to monitor the continuing trustworthiness of their personnel;

.6 ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material;

.7 knowledge of the requirements of SOLAS chapter XI-2 and part A of the ISPS Code and relevant national and international legislation and security requirements;

.8 knowledge of current security threats and patterns;

.9 knowledge on recognition and detection of weapons, dangerous substances and devices;

.10 knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.11 knowledge on techniques used to circumvent security measures; and

.12 knowledge of security and surveillance equipment and systems and their operational limitations.

2.5.2.2 When delegating specific duties to a recognized security organization, [the specified organization] should ensure that the recognized security organization has the competencies needed to undertake the task.

(ISPS Code, part B, paragraph 4.5)

2.5.3 Recognized security organizations – Authorities

2.5.3.1 [The specified organization] may authorize a recognized security organization to undertake certain security-related activities, including:

.1 approval of ship security plans, or amendments thereto, on behalf of the Administration;

.2 verification and certification of compliance of ships with the requirements of SOLAS chapter XI-2 and part A of the ISPS Code on behalf of the Administration; and

.3 conducting port facility security assessments required by the government.

2.5.3.2 A recognized security organization may also advise or provide assistance to companies or port facilities on security matters, including ship security assessments, ship security plans, port facility security assessments and port facility security plans. This can include completion of a ship security assessment or plan or port facility security assessment or plan.

(ISPS Code, part B, paragraphs 4.3 and 4.4)

2.5.4 Recognized security organizations – Restrictions

2.5.4.1 Recognized security organizations shall not:

.1 set the applicable security level;

.2 approve a port facility security assessment and subsequent amendments to an approved assessment;

.3 determine the port facilities which will be required to designate a port facility security officer;

.4 approve a port facility security plan and subsequent amendments to an approved plan;

.5 exercise control and compliance measures pursuant to SOLAS regulation XI-2/9;

.6 establish the requirements for a declaration of security; and

.7 approve, verify, or certify a work product that it has developed.

(ISPS Code, part A, paragraphs 4.3 and 9.2.1)
(MSC.1/Circ.1074)

2.5.5 Recognized security organizations oversight

2.5.5.1 Governments retain ultimate responsibility for the work undertaken on their behalf by the recognized security organizations that they appoint. They have the authority to modify or revoke their delegations to a recognized security organization which fails to meet agreed performance standards.

(GMSIC, paragraph 2.5.11)

2.6 Documentation

2.6.1 Security assessments

2.6.1.1 The ship and port facility security assessments are an essential and integral part of the process of developing and updating the ship and port facility security plans, respectively.

(ISPS Code, part A, paragraphs 8.1 and 15.1)

2.6.2 Security plans

2.6.2.1 The legislation should set out the requirements and the procedures applying to:

.1 the submission of port facility security plans and ship security plans;

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

.3 the requirements to review an approved port facility security plan and ship security plan;

.4 the submission of amendments to an approved port facility security plan and ship security plan; and

.5 consideration of any applications for exemptions from holding a plan, consistent with SOLAS regulation 1/4(a).

(SOLAS regulation I/4(a))
(GMSIC, paragraph 2.2.35)

2.6.3 Unauthorized disclosure

2.6.3.1 [The specified organization] should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to ship security assessments, ship security plans, port facility security assessments and port facility security plans, and to individual assessments or plans.

(ISPS Code, part B, paragraph 4.1)

2.6.4 Declarations of security

2.6.4.1 *[The specified organization]* shall determine when a declaration of security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment.

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

2.6.4.3 A ship may request completion of a declaration of security when:

.1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;

.2 there is an agreement on a declaration of security between governments covering certain international voyages or specific ships on those voyages;

.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

.4 the ship is at a port which is not required to have and implement an approved port facility security plan; or

.5 the ship is conducting ship-to-ship activities with another ship not required to have and implement an approved ship security plan.

(ISPS Code, part A, paragraphs 5.1, 5.2 and 5.5)

2.6.5 Records

2.6.5.1 Ships shall keep records of the last 10 calls at port facilities.

2.6.5.2 Records of the following activities shall be kept on board for the minimum period specified by [the specified organization]:

.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 in;

.6 internal audits and reviews of security activities;

.7 periodic review of the ship security assessment;

.8 periodic review of the ship security plan;

.9 implementation of any amendments to the plan; and

.10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

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

(SOLAS regulation XI-2/9.2.3)
(ISPS Code, part A, paragraphs 10.1 and 10.4)

2.6.6 Audits

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

(ISPS Code, part A, paragraph 9.4.1)

2.7 Security levels

2.7.1 Security levels – General

2.7.1.1 The three levels of risk are now used internationally:

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

.2 "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.

.3 "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.

(ISPS Code, part A, paragraph 2.1.9 – 2.1.11)

2.7.2 Security level 1

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

.1 ensuring the performance of all ship and/or port facility security duties;

.2 controlling access to the ship and/or port facility;

.3 controlling the embarkation of persons and their effects;

.4 monitoring of the ship deck and/or port facility, including anchoring and berthing area(s) and areas surrounding the ship;

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

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

.7 ensuring that security communication is readily available.

(ISPS Code, part A, paragraphs 7.2 and 14.2)

2.7.3 Security level 2

2.7.3.1 At security level 2, the additional protective measures, specified in the ship and/or port facility security plan, shall be implemented for each required activity, taking into account the guidance given in part B of the ISPS Code.

(ISPS Code, part A, paragraphs 7.3 and 14.3)

2.7.4 Security level 3

2.7.4.1 At security level 3, further specific protective measures, specified in the ship and/or port facility security plan, shall be implemented for each required activity, taking into account the guidance given in part B of the ISPS Code.

(ISPS Code, part A, paragraphs 7.4 and 14.4)

2.7.5 Security level coordination

2.7.5.1 Ships intending to enter a port or port facility should establish the applicable security level through direct contact with the port authority, or the Port Security Officer or the 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 Security Officer or the Port Facility Security Officer prior to entry.

2.7.5.2 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.

2.7.5.3 A ship can, however, operate at a higher security level 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.

(GMSIC, paragraphs 4.3.2, 4.3.3 and 4.3.4)

Part 3 – Ship security

3.1 Company Security Officer

3.1.1 Company Security Officer – General

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

(ISPS Code, part A, paragraph 11.1)

3.1.2 Company Security Officer – Qualifications

3.1.2.1 Every person designated as a Company Security Officer should be able to demonstrate competence to undertake the following tasks, duties and responsibilities.

3.1.2.2 The Company Security Officer and appropriate shore-based company personnel, should have knowledge of, and receive training in, some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of ship security assessment;

.6 methods of ship security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

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

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with port facilities; and

.20 assessment of security drills and exercises.

(ISPS Code, part B, paragraph 13.1)
(MSC.1/Circ.1154)

3.1.3 Company Security Officer – Duties

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

3.1.3.2 The duties and responsibilities of the Company Security Officer shall also include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and cooperation between the Ship Security Officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirements;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

(ISPS Code, part A, paragraphs 8.2 and 11.2)

3.2 Ship Security Officer

3.2.1 Ship Security Officer – General

3.2.1.1 A Ship Security Officer shall be designated on each ship.

(ISPS Code, part A, paragraph 12.1)

3.2.2 Ship Security Officer – Qualifications

3.2.2.1 Ship Security Officers shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of the ISPS Code.

3.2.2.2 The Ship Security Officer should have knowledge of, and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of ship security assessment;

.6 methods of ship security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

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

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with port facilities;

.20 assessment of security drills and exercises;

.21 the layout of the ship;

.22 the ship security plan and related procedures (including scenario-based training on how to respond);

.23 crowd management and control techniques;

.24 operations of security equipment and systems; and

.25 testing, calibration and whilst at sea maintenance of security equipment and systems.

(ISPS Code, part A, paragraph 13.3)
(ISPS Code, part B, paragraphs 13.1 and 13.2)

3.2.3 Ship Security Officer – Duties

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

.1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.2 maintaining and supervising the implementation of the Ship Security Plan, including any amendments to the plan;

.3 coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

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

.6 enhancing security awareness and vigilance on board;

.7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.8 reporting all security incidents;

.9 coordinating implementation of the ship security plan with the Company Security Officer and the relevant port facility security officer; and

.10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

(ISPS Code, part A, paragraph12.2)

3.3 Shipboard personnel

3.3.1 Shipboard personnel – Qualifications

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

3.3.1.2 Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

.1 knowledge of current security threats and patterns;

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

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 crowd management and control techniques;

.6 security-related communications;

.7 knowledge of the emergency procedures and contingency plans;

.8 operations of security equipment and systems;

.9 testing, calibration and whilst at sea maintenance of security equipment and systems;

.10 inspection, control, and monitoring techniques; and

.11 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

3.3.1.3 All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the ship security plan, including:

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

.2 knowledge of the emergency procedures and contingency plans;

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

.4 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and

.5 techniques used to circumvent security measures.

(ISPS Code, part A, paragraph 13.3)
(ISPS Code, part B, paragraphs 13.3 and 13.4)

3.4 Documentation

3.4.1 Ship security assessment

3.4.1.1 Company Security Officers are responsible for undertaking ship security assessments.

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

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

.2 identification and evaluation of key 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; and

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

3.4.1.3 The ship security assessment should also address the following elements on board or within the ship:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks; and

.6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

(ISPS Code, part A, paragraph 8.4)
(ISPS Code, part B, paragraph 8.3)
(GMSIC, paragraph 2.9.12)

3.4.2 Ship security plan

3.4.2.1 Each ship shall carry on board a ship security plan approved by the Administration, unless exempted. The plan shall make provisions for the three security levels as defined in part A of the ISPS Code.

3.4.2.2 The ship security plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

.9 procedures for training, drills and exercises associated with the plan;

.10 procedures for interfacing with port facility security activities;

.11 procedures for the periodic review of the plan and for updating;

.12 procedures for reporting security incidents;

.13 identification of the Ship Security Officer;

.14 identification of the Company Security Officer including 24-hour contact details;

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided; and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

3.4.2.3 The ship security plan shall be protected from unauthorized access or disclosure.

3.4.2.4 Ship security plans should be reviewed annually, or following:

.1 a major security drill or exercise;

.2 a security threat or incident involving the ship;

.3 a change in shipping operations, including the operator;

.4 completion of a review of the ship security assessment;

.5 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 ship security plan may no longer be relevant.

(ISPS Code, part A, paragraphs 9.1, 9.4 and 9.7)
(GMSIC, paragraph 2.9.23)

3.5 Training, drills and exercises

3.5.1 Training

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

3.5.1.1 Shipboard personnel without designated security duties should receive security-related familiarization training to be able to:

.1 report a security incident;

.2 know the procedures to follow when they recognize a security threat; and

.3 take part in security-related emergency and contingency procedures.

(ISPS Code, part A, paragraphs 13.1 and 13.2)
(MSC.1/Circ.1235)

3.5.2 Drills

3.5.2.1 Drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances.

3.5.2.2 Drills should *be conducted at least once every three months. In addition, where more than 25% of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship within the last three months, a drill should be conducted within one week of the change.*

3.5.2.3 Drills may be defined as supervised activities that are used to test a single measure or procedure in the ship security plan.

3.5.2.4 Shipboard drills should cover such scenarios as:

.1 identification and search of unauthorized visitors on board the ship;

.2 recognition of materials that may pose a security threat;

.3 methods to deter attackers from approaching the ship;

.4 recognition of restricted areas; and

.5 mustering for evacuation.

(ISPS Code, part A, paragraph 13.4)
(ISPS Code, part B, paragraph 13.6)
(GMSIC, paragraphs 4.8.13 and 4.8.15)

3.5.3 Exercises

3.5.3.1 The Company Security Officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals.

3.5.3.2 Exercises should be carried out at least once each calendar year with no more than 18 months between the exercises.

3.5.3.3 Exercises are more complex activities which test several measures and procedures at the same time.

3.5.3.4 Exercises should test communications, coordination, resource availability, and response. Exercises may be:

.1 full scale or live;

.2 table top simulation or seminar; or

.3 combined with other exercises held such as search and rescue or emergency response exercises.

(ISPS Code, part A, paragraph 13.5)
(ISPS Code, part B, paragraph 13.7)
(GMSIC, paragraph 4.8.13)

3.6 Physical security

3.6.1 Restricted areas

3.6.1.1 The ship security plan shall address the identification of the restricted areas and measures for the prevention of unauthorized access to them.

3.6.1.2 The ship security plan should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 prevent unauthorized access;

.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;

.3 protect sensitive security areas within the ship; and

.4 protect cargo and ship's stores from tampering.

3.6.1.3 Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in SOLAS chapter XI-2;

.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

.3 ventilation and air-conditioning systems and other similar spaces;

.4 spaces with access to potable water tanks, pumps, or manifolds;

.5 spaces containing dangerous goods or hazardous substances;

.6 spaces containing cargo pumps and their controls;

.7 cargo spaces and spaces containing ship's stores;

.8 crew accommodation; and

.9 any other areas as determined by the Company Security Officer, through the ship security assessment to which access must be restricted to maintain the security of the ship.

(ISPS Code, part A, paragraph 9.4.2)
(ISPS Code, part B, paragraphs 9.18 and 9.21)

3.6.2 Access points

3.6.2.1 The ship security plan shall address measures for the prevention of unauthorized access to the ship, including boarding of a ship when in port or at sea.

(ISPS Code, part A, paragraph 9.4)

3.6.3 Signage

3.6.3.1 The ship security plan should ensure that all restricted areas should be clearly marked, indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

(ISPS Code, part B, paragraph 9.20)

3.6.4 Identification

3.6.4.1 The ship security plan should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge.

(ISPS Code, part B, paragraph 9.11)

3.6.5 Lighting

3.6.5.1 The ship should have lighting sufficient to monitor the ship, the restricted areas on board and areas surrounding the ship.

(ISPS Code, part B, paragraph 9.42)

3.6.6 Surveillance

3.6.6.1 The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of: watchkeepers, security guards and deck watches including patrols.

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

.1 closed-circuit television (CCTV) and lighting;

.2 communications and x-ray equipment;

.3 archway and hand-held metal detectors;

.4 perimeter/intruder detection systems;

.5 automated access control equipment;

.6 information, including computer, security; and

.7 explosive trace and vapour detection equipment.

(ISPS Code, part B, paragraph 9.42)
(GMSIC, paragraph 2.9.41)

3.6.7 Communications

3.6.7.1 Ship Security Officers intending to use a port facility should maintain effective communication with the Port Facility Security Officers (PFSOs).

(GMSIC, paragraph 2.8.19)

3.7 Operational security

3.7.1 Master's discretion

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

3.7.1.2 If, in the professional judgment of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship.

(SOLAS regulations XI-2/8.1 and 8.2)

3.7.2 Port control compliance

3.7.2.1 Every ship intending to enter a port facility of [State] shall provide the security information requested by the officers duly authorized by that government. The master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

(SOLAS regulation XI-2/9.2.2)

3.7.3 Manning requirements

3.7.3.1 In establishing the minimum safe manning of a ship the Administration should take into account any additional workload which may result from the implementation of the ship security plan and ensure that the ship is sufficiently and effectively manned.

(ISPS Code, part B, paragraph 4.28)

3.7.4 Access control

3.7.4.1 Ship security plans shall address measures for the prevention of unauthorized access to the ship.

(ISPS Code, part A, paragraph 9.4.3)

3.7.5 Cargo operations

3.7.5.1 Security measures relating to cargo handling should:

.1 prevent tampering; and

.2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

3.7.5.2 Cargo entering the port facility should have adequate and reliable documentation, which is standardized, matches the cargo with the conveyance transporting it to the port facility, is resistant to forgery and is consistently examined by security personnel prior to allowing admittance onto the port facility.

(ISPS Code, part B, paragraph 9.25)
(GMSIC, paragraph 3.8.23)

3.7.6 Ship's stores

3.7.6.1 Security measures relating to the delivery of ship's stores should:

.1 ensure the integrity of ship's stores;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering; and

.4 prevent ship's stores from being accepted unless ordered.

3.7.6.2 Ship's stores entering the port facility should have adequate and reliable documentation, which is standardized, matches the ship's stores with the conveyance transporting it to the port facility, is resistant to forgery and is consistently examined by security personnel prior to allowing admittance onto the port facility.

(ISPS Code, part B, paragraph 9.33)
(GMSIC, paragraph 3.8.23)

3.7.7 Unaccompanied baggage procedures

3.7.7.1 The ship security plan should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship.

(ISPS Code, part B, paragraph 9.38)

3.8 Security obligations

3.8.1 International Ship Security Certificate (ISSC)

3.8.1.1 Ships shall carry on board either the International Ship Security Certificate or, in limited circumstances, the Interim International Ship Security Certificate, both of which are issued by [the specified organization].

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

.1 the ship security assessment required by the ISPS Code has been completed;

.2 a copy of the ship security plan meeting the requirements of SOLAS chapter XI-2 and part A of the ISPS Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;

.3 the ship is provided with a ship security alert system meeting the requirements of SOLAS regulation XI-2/6, if required;

.4 the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in part A of the ISPS Code; and

.5 the Ship Security Officer meets the requirements of part A of the ISPS Code.

3.8.1.3 An International Ship Security Certificate shall not be valid for more than five years.

3.8.1.4 A ship which is not normally engaged on international voyages but which, in exceptional circumstances, is required to undertake a single international voyage may be exempted by [the specified organization] from any of the requirements of the present regulations provided that it complies with safety requirements which are adequate in the opinion of [the specified organization] for the voyage which is to be undertaken by the ship.

(SOLAS regulations I/4(a) and XI/2.9.1)
(ISPS Code, part A, paragraphs 19.3.1 and 19.4.2)
(GMSIC, paragraph 4.9.1)

3.8.2 Communications/reporting procedures

3.8.2.1 Ships intending to enter ports of [State] may be required to provide the following information prior to entry into port:

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

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

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

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

.5 that the appropriate ship security procedures were maintained during any ship-to-ship activity within a specified time frame; or

.6 other practical security-related information (not to include details of the ship security plan).

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

.1 information contained in the continuous synopsis record;

.2 location of the ship at the time the report is made;

.3 expected time of arrival of the ship in port;

.4 crew list;

.5 general description of cargo aboard the ship;

.6 passenger list; and

.7 information required to be carried under SOLAS regulation XI-2/5.

3.8.2.3 [The Specified organization] may specify 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.

3.8.2.4 The master may decline to provide such information, but failure to do so may result in denial of entry into port.

(SOLAS regulation XI-2/9.2.1)
(ISPS Code, part B, paragraph 4.39)
(GMSIC, paragraphs 2.11.8 and 4.6.14)

3.9 Incident response

3.9.1 Security incidents

3.9.1.1 [The specified organization] is 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. They should include reporting incidents to local law-enforcement agencies when in a port facility or the adjacent coastal State.

3.9.1.2 Security incidents generally can fall into two categories:

.1 those considered to be sufficiently serious that they should be reported to relevant authorities by the Company Security Officer, including:

.1 unauthorized access to restricted areas within the ship for suspected threat-related reasons;

.2 unauthorized carriage or discovery of stowaways, weapons or explosives;

.3 incidents of which the media are aware;

.4 bomb warnings;

.5 attempted or successful boardings; and

.6 damage to the ship caused by explosive devices or arson.

.2 those of a less serious nature but which require reporting to, and investigation by, the Ship Security Officer can include:

.1 unauthorized access to the ship caused by breaches of access control points;

.2 inappropriate use of passes;

.3 damage to equipment through sabotage or vandalism;

.4 unauthorized disclosure of a ship security plan;

.5 suspicious behaviour near the ship when at a port facility;

.6 suspicious packages near the ship when at a port facility; and

.7 unsecured access points to the ship.

(GMSIC, paragraphs 2.9.37 and 4.8.35)

3.9.2 Unauthorized access/breach procedures

3.9.2.1 Ship security plans shall address procedures for responding to security threats or breaches of security, including:

.1 provisions for maintaining critical operations of the ship or ship/port interface; and

.2 procedures for reporting security incidents.

(ISPS Code, part A, paragraphs 9.4.4 and 9.4.12)

3.9.3 Best management practices

3.9.3.1 The Company Security Officer is encouraged to ensure that a ship security plan is in place for passage through high security risk areas, and that this is exercised, briefed and discussed with the Master and the Ship Security Officer.

3.9.3.2 The provision of carefully planned and installed ship protection measures prior to transiting the high risk area is very strongly recommended.

3.9.3.3 Ship security plans 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.

(MSC.1/Circ.1339, paragraphs 6.4 and 6.7)
(GMSIC, paragraph 2.9.30)

Part 4 – Port facility security

4.1 Port Facility Security Officer

4.1.1 Port Facility Security Officer – general

4.1.1.1 A Port Facility Security Officer shall be designated for each port facility. A person may be designated as the Port Facility Security Officer for one or more port facilities.

(ISPS Code, part A, paragraph 17.1)

4.1.2 Port Facility Security Officer – qualifications

4.1.2.1 The Port Facility Security Officer should have knowledge and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of port facility security assessment;

.6 methods of ship and port facility security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

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

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems, and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with ships; and

.20 assessment of security drills and exercises.

4.1.2.2 The Port Facility Security Officer 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.

(ISPS Code, part B, paragraph 18.1)
(GMSIC, paragraph 2.2.29.3)

4.1.3 Port Facility Security Officer – Duties

4.1.3.1 The duties and responsibilities of the Port Facility Security Officer shall include, but are not limited to:

.1 conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;

.2 ensuring the development and maintenance of the port facility security Plan;

.3 implementing and exercising the port facility security plan;

.4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;

.5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;

.6 enhancing security awareness and vigilance of the port facility personnel;

.7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;

.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;

.9 coordinating implementation of the port facility security plan with the appropriate company and Ship Security Officer(s);

.10 coordinating with security services, as appropriate;

.11 ensuring that standards for personnel responsible for security of the port facility are met;

.12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

.13 assisting Ship Security Officers in confirming the identity of those seeking to board the ship when requested.

(ISPS Code, part A, paragraph 17.2)

4.2 Port Security Committee

4.2.1 Port Security Committee – General

4.2.1.1 Port operators may establish port security committees to coordinate the implementation of the maritime security measures in their port in a consistent manner.

(GMSIC, paragraph 2.8.17)

4.3 Documentation

4.3.1 Port facility security assessment

4.3.1.1 The port facility security assessment shall be carried out by [the *specified* organization]. The government may authorize a recognized security organization to carry out the port facility security assessment of a specific port facility located within its territory.

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

.1 identification and evaluation of important assets and infrastructure it is important to protect;

.2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

.3 identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and

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

(ISPS Code, part A, paragraphs 15.2 and 15.5)

4.3.2 Port facility security plan

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

4.3.2.2 Such a plan shall address, at least, the following:

.1 measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;

.2 measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

.3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;

.4 procedures for responding to any security instructions the contracting government, in whose territory the port facility is located, may give at security level 3;

.5 procedures for evacuation in case of security threats or breaches of security;

.6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;

.7 procedures for interfacing with ship security activities;

.8 procedures for the periodic review of the plan and updating;

.9 procedures for reporting security incidents;

.10 identification of the port facility security officer including 24-hour contact details;

.11 measures to ensure the security of the information contained in the plan;

.12 measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

.13 procedures for auditing the port facility security plan;

.14 procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

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

4.3.2.3 [The specified organization] should take the human element, the need to afford special protection to seafarers and the critical importance of shore leave into account when implementing the provisions of SOLAS chapter XI-2 and the ISPS Code.

4.3.2.4 [The specified organization] should establish appropriate procedures to provide for:

.1 the submission of port facility security plans to them;

.2 the consideration of port facility security plans;

.3 the approval of port facility security plans, with or without amendments;

.4 consideration of amendments submitted after approval; and

.5 procedures for inspecting or auditing the continuing relevance of the approved port facility security plan.

4.3.2.5 At all stages steps should be taken to ensure that the contents of the port facility security plan remains confidential.

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

(Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, Conference Resolution 11)
(ISPS Code, part A, paragraphs 16.1, 16.3 and 16.4)
(ISPS Code, part B, paragraph 16.61

4.3.3 Statement of compliance

4.3.3.1 [The specified organization] may issue an appropriate Statement of compliance of a port facility indicating:

.1 the port facility;

.2 that the port facility complies with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code;

.3 the period of validity of the Statement of compliance of a port facility which should be specified by the government but should not exceed five years; and

.4 the subsequent verification arrangements established by the government and a confirmation when these are carried out.

4.3.3.2 A Statement of compliance should not be issued unless the Designated Authority has confirmed that:

.1 the port facility has a port facility security assessment undertaken, or approved, by the Designated Authority;

.2 the port facility has a port facility security plan which has been duly and formally approved by the Designated Authority;

.3 the port facility's security staff have received the necessary training and can implement the security procedures in the approved port facility security plan; and

.4 any security equipment specified in the port facility security plan is in place and operating effectively.

(ISPS Code, part B, paragraph 16.62)
(GMSIC, paragraph 2.8.53)

4.4 Training, drills and exercises

4.4.1 Basic port security knowledge

4.4.1.1 Port facility personnel should receive adequate security-related training or instruction and familiarization training to perform their assigned duties.

4.4.1.2 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.

(MSC.1/Circ.1341)
(GMSIC, paragraph 3.5.7)

4.4.2 Training

4.4.2.1 The Port Facility Security Officer and appropriate port facility personnel shall have knowledge and have received training, taking into account the guidance given in part B of the ISPS Code.

4.4.2.2 The Port Facility Security Officer should have knowledge and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of port facility security assessment;

.6 methods of ship and port facility security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

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

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems, and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with ships; and

.20 assessment of security drills and exercises.

4.4.2.3 Port facility personnel having specific security duties should have knowledge and receive training, in some or all of the following, as appropriate:

.1 knowledge of current security threats and patterns;

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

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 crowd management and control techniques;

.6 security-related communications;

.7 operations of security equipment and systems;

.8 testing, calibration and maintenance of security equipment and systems;

.9 inspection, control, and monitoring techniques; and

.10 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

4.4.2.4 All other port facility personnel should have knowledge of and be familiar with relevant provisions of the port facility security plan, in some or all of the following, as appropriate:

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

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

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and

.4 techniques used to circumvent security measures.

(ISPS Code, part A, paragraph 18.1)
(ISPS Code, part B, paragraphs 18.1, 18.2 and 18.3)

4.4.3 Drills

4.4.3.1 Drills shall be carried out at appropriate intervals taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances.

4.4.3.2 Drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan addressing specific security threats.

4.4.3.3 Drills may be defined as supervised activities that are used to test a single measure or procedure in the port facility security plan.

(ISPS Code, part A, paragraph 18.3)
(ISPS Code, part B, paragraph 18.5)
(GMSIC, paragraph 4.8.13)

4.4.4 Exercises

4.4.4.1 The Port Facility Security Officer shall participate in security exercises at appropriate intervals.

4.4.4.2 Exercises which may include the participation of Port Facility Security Officers, and other relevant authorities should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises may be:

.1 full scale or live;

.2 table top simulation or seminar; or

.3 combined with other exercises held such as emergency response or other port State authority exercises.

4.4.4.3 Exercises are more complex activities which test several measures and procedures at the same time.

(ISPS Code, part A, paragraph 18.4)
(ISPS Code, part B, paragraph 18.6)
(GMSIC, paragraph 4.8.13)

4.5 Physical security

4.5.1 Port facility security measures

4.5.1.1 Security measures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

(ISPS Code, part A, paragraph 14.1)

4.5.2 Physical security – general

4.5.2.1 [The specified organization] may set standards for the installation and maintenance of port facility security equipment. Such standards may address:

.1 fencing, gates, vehicle barriers and lighting;

.2 closed-circuit television (CCTV);

.3 communications and x-ray equipment;

.4 archway and hand-held metal detectors;

.5 perimeter/intruder detection systems;

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

.7 information and computer protection systems; and

.8 explosive trace and vapour detection equipment.

(GMSIC, paragraph 2.8.50)

4.5.3 Restricted areas

4.5.3.1 Port facility security plans shall address measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility.

4.5.3.2 The port facility security plan should identify the restricted areas to be established within the port facility and specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas is to:

.1 protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;

.2 protect the port facility;

.3 protect the ships using, and serving, the port facility;

.4 protect security-sensitive locations and areas within the port facility;

.5 protect security and surveillance equipment and systems; and

.6 protect cargo and ship's stores from tampering.

4.5.3.3 Restricted areas may include:

.1 shore and waterside areas immediately adjacent to the ship;

.2 embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas including search points;

.3 areas where loading, unloading or storage of cargo and stores is undertaken;

.4 locations where security sensitive information, including cargo documentation, is held;

.5 areas where dangerous goods and hazardous substances are held;

.6 vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;

.7 areas where security and surveillance equipment are stored or located;

.8 essential electrical, radio and telecommunication, water and other utility installations; and

.9 other locations in the port facility where access by vessels, vehicles and individuals should be restricted.

(ISPS Code, part A, paragraph 16.3.2)
(ISPS Code, part B, paragraphs 16.21 and 16.25)

4.5.4 Perimeter

4.5.4.1 The port facility security plan should establish restricted areas which should be bound by fencing or other barriers to a standard which should be approved by [the specified organization].

(ISPS Code, part B, paragraph 16.17.1)

4.5.5 Signage

4.5.5.1 The port facility security plans should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

(ISPS Code, part B, paragraph 16.23)

4.5.6 Access points

4.5.6.1 The port facility security plan should establish the security measures covering all means of access to the port facility.

4.5.6.2 The port facility security plan should establish the control points restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity.

(ISPS Code, part B, paragraphs 16.10 and 16.17.5)

4.5.7 Communications

4.5.7.1 Port facility security plans shall address procedures for interfacing with ship security activities.

(ISPS Code, part A, paragraph 16.3.7)

4.5.8 Surveillance

4.5.8.1 The port facility security organization should have the capability to monitor the port facility and its nearby approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:

.1 lighting;

.2 security guards, including foot, vehicle and waterborne patrols; and

.3 automatic intrusion detection devices and surveillance equipment.

(ISPS Code, part B, paragraph 16.49)

4.6 Operational security

4.6.1 Access control

4.6.1.1 The port facility security plan should ensure that all restricted areas have clearly established security measures to control:

.1 access by individuals;

.2 the entry, parking, loading and unloading of vehicles;

.3 movement and storage of cargo and ship's stores; and

.4 unaccompanied baggage or personal effects.

(ISPS Code, part B, paragraph 16.22)

4.6.2 Identification

4.6.2.1 The port facility security plan should establish the control points to check identity of all persons seeking entry to the port facility in connection with a ship.

4.6.2.2 The port facility security plan should establish for each security level the means of identification required to allow access to the port facility for port facility personnel and for visitors respectively.

4.6.2.3 Any port facility identification system should, when it is practicable to do so, be coordinated with that applying to ships that regularly use the port facility.

(ISPS Code, part B, paragraphs 16.12 and 16.17.2)

4.6.3 Access control – Visitors

4.6.3.1 The port facility security plan should establish the control points to check identity of passengers, ship's personnel and visitors and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc.

4.6.3.2 A document exchange may be utilized whereby the visitor must surrender a Government-issued identity document in exchange for a visitor pass that must be displayed.

(ISPS Code, part B, paragraph 16.17.2)
(GMSIC, paragraph 3.8.22.4)

4.6.4 Access control – Vehicles

4.6.4.1 The port facility security plan should establish the control points to check vehicles used by those seeking entry to the port facility in connection with a ship.

(ISPS Code, part B, paragraph 16.17.3)

4.6.5 Access control – Cargo

4.6.5.1 The port facility security plan should establish inventory control procedures at access points to the port facility. Once within the port facility, cargo should be capable of being identified as having been checked and accepted for loading onto the ship or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

(ISPS Code, part B, paragraph 16.31)

4.6.6 Access control – Ship's stores

4.6.6.1 The port facility security plan may establish procedures involving ships regularly using the port facility, including their suppliers and the port facility covering notification and timing of deliveries and their documentation. Stores presented for delivery should be accompanied by evidence that they have been ordered by the ship.

(ISPS Code, part B, paragraph 16.39)

4.6.7 Access control – Passengers

4.6.7.1 Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised.

4.6.7.2 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the port facility.

(ISPS Code, part B, paragraphs 16.12 and 16.13)

4.6.8 Access control – Ship's crew

4.6.8.1 The port facility security plan shall address 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.

4.6.8.2 Foreign crew members should be allowed ashore by the public authorities while the ship on which they arrive is in port, provided that the formalities on arrival of the ship have been fulfilled and there is no reason to refuse permission to come ashore for reasons of public health, public safety or public order.

(ISPS Code, part A, paragraph 16.3.15)
(Resolution A.1090(28))

4.6.9 Searches

4.6.9.1 The port facility security plan should establish the control points where searches of persons, personal effects, vehicles and their contents may be applied.

4.6.9.2 All those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the port facility security plan.

(ISPS Code, part B, paragraphs 16.17.6 and 16.18)

4.6.10 Cargo operations

4.6.10.1 Port facility security plans shall address measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility.

4.6.10.2 The security measures relating to cargo handling should:

.1 prevent tampering; and

.2 prevent cargo that is not meant for carriage from being accepted and stored within the port facility.

4.6.10.3 Security measures to be applied during cargo handling may include:

.1 routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;

.2 checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;

.3 searches of vehicles; and

.4 checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

4.6.10.4 Checking of cargo may be accomplished by some or all of the following means:

.1 visual and physical examination; and

.2 using scanning/detection equipment, mechanical devices, or dogs.

(ISPS Code, part A, paragraph 16.3.12)
(ISPS Code, part B, paragraphs 16.30, 16.32 and 16.33)

4.6.11 Ship's stores

4.6.11.1 The port facility security plan should establish the security measures relating to the delivery of ship's stores to:

.1 ensure checking of ship's stores and package integrity;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering;

.4 prevent ship's stores from being accepted unless ordered;

.5 ensure searching the delivery vehicle; and

.6 ensure escorting delivery vehicles within the port facility.

(ISPS Code, part B, paragraph 16.38)

4.6.12 Unaccompanied baggage procedures

4.6.12.1 The port facility security plan should establish the security measures to ensure that unaccompanied baggage is identified and subjected to appropriate screening, including searching, before it is allowed in the port facility or transferred between the port facility and the ship.

(ISPS Code, part B, paragraph 16.45)

4.7 Incident response

4.7.1 Port security incidents

4.7.1.1 Port facility security plans shall address procedures for responding to breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface, and procedures for reporting security incidents.

4.7.1.2 Security incidents generally fall into two categories:

.1 those considered to be sufficiently serious that they should be reported to relevant authorities by the Port Facility Security Officer, including:

.1 unauthorized access to restricted areas within the port facility;

.2 unauthorized carriage or discovery of weapons or prohibited items in the port facility;

.3 incidents of which the media are aware;

.4 bomb warnings; and

.5 unauthorized disclosure of a port facility security plan.

.2 those of a less serious nature but which require reporting to, and investigation by, the Port Facility Security Officer, including:

.1 breaches of screening points;

.2 inappropriate uses of passes;

.3 damage to security equipment through sabotage or vandalism;

.4 suspicious behaviour in or near the port facility;

.5 suspicious packages in or near the port facility; and

.6 unsecured access points.

(ISPS Code, part A, paragraphs 16.3.3 and 16.3.9)
(GMSIC, paragraph 3.8.9)

4.7.2 Incident reporting requirements

4.7.3.1 Port facility security plans shall address procedures for reporting security incidents and PFSOs are required to report them to relevant authorities.

(GMSIC, paragraph 3.8.8)

Part 5 – Enforcement

Essential to the successful implementation and oversight of the ISPS Code is the drafting and enactment of appropriate national legislation to provide for the full implementation and oversight of the maritime security measures. The legislation should specify the powers needed for government officials to undertake the application of enforcement actions to correct incidents of non-compliance.

(GMSIC, paragraphs 2.2.1 and 2.2.3)

5.1 Control measures

5.1.1 Ship control measures

5.1.1.1 When there are clear grounds, or where no valid International Ship Security Certificate is produced when required, the officers duly authorized by [STATE] shall impose any one or more of the following control measures:

.1 inspection of the ship;

.2 delaying the ship;

.3 detention of the ship;

.4 restriction of operations, including movement within the port; or

.5 expulsion of the ship from port.

5.1.1.2 Such control measures may additionally or alternatively include other lesser administrative or corrective measures.

(SOLAS regulations XI-2/9.1.2 and 9.1.3)

5.1.2 Conditions of entry

5.1.2.1 [The specified organization] may require from a ship additional information as a condition of entry into port. Examples could include:

.1 records of the measures taken while visiting a port facility located in the territory of another State;

.2 declarations of security that were entered into with port facilities or other ships;

.3 confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility;

.4 records of the measures taken while engaged in a ship-to-ship activity with a ship flying the flag of a State which is not a Contracting Government to SOLAS especially those measures that would normally have been provided by ships flying the flag of SOLAS Contracting Governments;

.5 information contained in the continuous synopsis record;

.6 location of the ship at the time the report is made;

.7 expected time of arrival of the ship in port;

.8 crew list;

.9 general description of cargo aboard the ship; and

.10 passenger list.

(ISPS Code, part B, paragraphs 4.37-4.39)

5.2 Administrative enforcement

5.2.1 Administrative violations

5.2.1.1 This legislation should establish administrative or civil penalties when an individual, port facility or ship fails to comply with an administrative or civil enforcement notice.

(GMSIC, paragraph 2.2.45)

5.2.2 Administrative remedies

5.2.2.1 Security failings on a port facility or ship may lead to the:

.1 suspension or withdrawal of the approved port facility security plan, and the Statement of compliance if one has been issued; or

.2 suspension or withdrawal of the approved ship security plan and International Ship Security Certificate.

5.2.2.2 Where none of the preceding steps has resulted in correction of the deficiency, [STATE] may commence proceedings to seek sanctions against the port facility or ship operator.

5.2.2.3 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.

(GMSIC, paragraphs 2.15.21, 2.15.24 and 2.15.25)

5.2.3 Administrative appeals

5.2.3.1 Operators of port facilities and ships should be allowed 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 port facility security plans or ship security plans.

(GMSIC, paragraph 2.2.44)

5.3 Criminal enforcement

5.3.1 General

5.3.1.1 [State] shall promulgate all laws, decrees, orders and regulations and take all other steps necessary to give full and complete effect to the security directives of the Administration and Designated Authority in accordance with [State] constitution and laws.

(SOLAS art. I(b))

5.3.2 Criminal violations

5.3.2.1 [*State]'s legislation should establish criminal penalties when an individual, port facility or ship fails to comply with a criminal enforcement notice.*

5.3.2.2 It may be an offence to:

.1 fail to comply with an enforcement notice;

.2 intentionally obstruct or impersonate a government official, or other person acting on behalf of a Designated Authority or Administration;

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

.3 provide information known to be false to a government official, or other person acting on behalf of a Designated Authority or Administration; and

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

(GMSIC, paragraphs 2.2.45 and 2.2.51)

APPENDIX

SOURCES

1 Safety of Life at Sea Convention, 1974, as amended (SOLAS).

2 International Ship and Port Facility Security (ISPS) Code.

3 MSC.1/Circ.1074 – Interim Guidelines for the authorization of Recognized Security Organizations acting on behalf of the Administration and/or Designated Authority of a Contracting Government.

4 MSC.1/Circ.1154 – Guidelines on Training and certification for Company Security Officers.

5 MSC.1/Circ.1235 – Guidelines on Security-related training and familiarization for shipboard personnel.

6 MSC.1/Circ.1339 – Piracy and armed robbery against ships in waters off the Coast of Somalia – Best Management Practices for protection against Somalia based piracy.

7 MSC.1/Circ.1341 – Guidelines on Security-related training and familiarization for port facility personnel.

8 Resolution A.1090(28) – Fair treatment of crew members in respect of shore leave and access to shore-side facilities.

9 IMO "Guide to Maritime Security and the ISPS Code" (GMSIC) 2012 Edition.