



Ref. T2-MSS/2.11.1

MSC.1/Circ.1217
14 December 2006

**INTERIM GUIDANCE ON VOLUNTARY SELF-ASSESSMENT
BY COMPANIES AND COMPANY SECURITY OFFICERS (CSOs)
FOR SHIP SECURITY**

- 1 The Maritime Safety Committee (the Committee), at its eighty-second session (29 November to 8 December 2006), developed Interim Guidance on voluntary self-assessment by Companies and CSOs for ship security in an effort to assist Companies in the implementation of, and the maintenance of compliance with, the requirements of SOLAS chapter XI-2 and the ISPS Code.
- 2 The methodologies set out in the annex are designed solely for use by Companies and CSOs in conducting internal voluntary self-assessments.
- 3 The Committee agreed that the Voluntary self-assessment tool for Companies and CSOs for ship security is not a document which can be requested or required to be produced during the exercise of Control pursuant to the provisions of SOLAS regulation I/19, Control and Compliance measures pursuant to the provisions of SOLAS regulation XI-2/9, or by Administrations. In addition, the Committee agreed that those duly authorized by SOLAS Contracting Governments to exercise Control or Control and compliance measures are not vested with any authority to request or require the production from any ship or Company of the Voluntary self-assessment tool for Companies and CSOs for ship security.
- 4 Administrations are invited to bring the attached Interim Guidance to the attention of owners and Companies operating ships entitled to fly their flag and of Company security officers.
- 5 Administrations, international organizations and non-governmental organizations with consultative status are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the Interim Guidance for consideration of action to be taken.

ANNEX**INTERIM GUIDANCE ON VOLUNTARY SELF-ASSESSMENT
BY COMPANIES AND COMPANY SECURITY OFFICERS (CSOs) FOR SHIP SECURITY**

1 SOLAS chapter XI-2 and the ISPS Code have, *inter alia*, placed responsibilities on Companies for ship security. The provisions entered into force on 1 July 2004 and the appendix to this document provides guidance on a method of self-assessing the effectiveness with which a Company has fulfilled, and continues to fulfil, its obligations in respect of ship security such as the implementation of ship security plans and the relevant security measures in them.

2 Self-assessment by Companies and CSOs using the self-assessment tool could be undertaken with the support of experts, if appropriate.

3 Anyone undertaking the self-assessment should, at least, have knowledge of:

- .1 the requirements of SOLAS chapter XI-2 and the ISPS Code, including the related guidance developed by the Organization;
- .2 general security principles; and
- .3 the operation of ships.

4 The process and the completed self-assessment should be protected from unauthorized access or disclosure.

5 The effective implementation of ship security measures is a continuing responsibility. It is suggested that Companies self-assess their processes post-implementation and thereafter at least on a two yearly basis.

6 Anyone undertaking the self-assessment should consider using this tool in conjunction with the Guidance on voluntary self-assessment by Administrations and for ship security (MSC.1/Circ.1193 dated 30 May 2006).

Appendix: Voluntary self-assessment tool for Companies and company security officers for ship security.

APPENDIX

VOLUNTARY SELF-ASSESSMENT TOOL FOR COMPANIES AND COMPANY SECURITY OFFICERS (CSOs) FOR SHIP SECURITY

This Voluntary self-assessment tool for Companies and CSOs for ship security (Voluntary self-assessment tool) can be used to examine the status of implementation SOLAS chapter XI-2 and the ISPS Code by Companies.

This Voluntary self-assessment tool will help to identify any aspects of SOLAS chapter XI-2 and the ISPS Code that the company and CSO can address to enhance the SOLAS chapter XI-2 and ISPS Code implementation process.

SOLAS chapter XI-2 and part A of the ISPS Code, establish mandatory requirements for the implementation of the ISPS Code by Companies.

When using this Voluntary self-assessment tool, the person conducting the voluntary self-assessment should consider SOLAS chapter XI-2, ISPS Code part A and part B, as applicable in accordance with national legislation, and the related guidance developed by the Organization.

The following section should be completed prior to completing the tool. It can be used by the Company and its CSO(s) and will help to establish an overview of their performance in ship(s) security implementation.

Sufficiently detailed answers will prevent the drawing of erroneous conclusions when undertaking subsequent voluntary self assessments. It will also assist in the resolution of any doubts when subsequent self assessments are conducted by different persons.

Name of Company	Address of the Company
Name(s) of the CSO(s)	

Complete separate table for each CSO as appropriate

Name of CSO	
Does the CSO hold an appropriate training certificate?	
Was this training certificate submitted to the Administration for recognition?	

List of ship(s)

Name of the 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 using the Voluntary self-assessment tool:

- *Not all of the questions on the Voluntary self-assessment tool apply, or are relevant, to all types or sizes of ships. Some of these apply only in relation to specific types of ships. In such cases, the non-applicability of the particular question should be recorded in the 'Comments' box.*
- *When completing the Voluntary self-assessment tool, the 'Comments' box provides space for amplification where the 'Other' option is selected. However, experience has shown that it is also helpful to use 'Comments' box in cases where a 'No' answer has been recorded, thus giving an explanation of why not and details of any measures or procedures in place. Suggested actions should be recorded in the 'Recommendations' section of the Voluntary self-assessment tool.*

- *For the questions which have multiple options (for example questions 4.1 and 4.4), the 'Yes/No/Other' tick boxes should be replaced by a single column of boxes, which should be ticked as appropriate. This will be of benefit in cases where a 'No' answer may erroneously be taken as indicative of a non-compliance. Further explanation of any measures and procedures in place should be given in the 'Comments' box and any suggested actions should be recorded in the 'Recommendations' section of the Voluntary self-assessment tool.*
- *Ensure that one of the boxes is ticked for each question.*
- *If you ticked 'Yes', but the measures/procedures are not documented in the SSP(s) of the ship(s) being assessed, please enter a short description of them in the 'Comments' box.*
- *If you ticked the 'No' response against Part A questions, please describe the reason in the 'Comments' box.*
- *If you ticked 'Other' against Part B questions, please enter a short description in the comment box. 'Other' could include instances where alternative agreements or equivalent arrangements have been implemented.*
- *Please tick 'Other' if the question is not applicable and add 'n/a' in the 'Comments' box.*
- *If alternative measures/procedures from those listed in the ISPS Code are used, please enter a short description in the 'Comments' box.*
- *If work to implement the measures outlined in Part B or any alternative solutions is still in progress, a work schedule should be entered into the 'Comments' box.*
- *If there is not enough space in the comment box, assessors should continue the answer on a separate page. The relevant question number should be added in these circumstances as a reference aid.*
- *'Recommendation' boxes should be used to record any identified deficiencies and how these could be mitigated.*
- *The 'Outcome of Voluntary Self-Assessment' box should be used to provide a brief record of the assessment process, and along with the comments in the 'Recommendation' boxes, form the basis for future security planning. A schedule for the implementation of recommendations should be included.*

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:			
.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:			
.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:			
.3 Does the CSO inform the Administration of SSAS implementation details and alterations? (SOLAS regulation XI-2/6.2.1)	☐	☐	☐
Comments:			
.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:			
.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)	☐	☐	☐
Comments:			
.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:			
.5 Does the Company update and keep the information provided current as and when changes occur? (ISPS Code, paragraph B/6.2)	☐	☐	☐
Comments:			
.6 Is the information provided in the English, French or Spanish language? (ISPS Code, paragraph B/6.3)	☐	☐	☐
Comments:			
.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:			

.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.1130? (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:			

	Yes	No	Other
.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)

Part A	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:			
.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:			
.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)

.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:			

.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 Ship security assessment (ISPS Code, paragraphs B/8.3, B/8.4, B/8.6 to B/8.13)

	Yes	No	Other
.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:			

	Yes	No	Other
.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:			
-----------	--	--	--

	Yes	No	Other
--	-----	----	-------

.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:			

	Yes	No	Other
.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)

Part A		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:				
.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:				
.4	Is an English, French or Spanish language version also available? (ISPS Code, section A/9.4)	☐	☐	☐
Comments:				
.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 of 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 (ISPS Code, paragraphs B/9.1 to 9.5)

	Yes	No	Other
.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:			
.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:				
.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?	☐	☐	☐
.13	Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships, in accordance with SOLAS regulations XI-2/11 and XI-2/12, are implemented and maintained?	☐	☐	☐

Comments:			
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)

Part A	Yes	No	Other
.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:			
.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)

Part B		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 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?	☐	☐	☐
Comments:				
.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:				

Part B		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:				
.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:				
.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)

		Yes	No	Other
.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 voluntary self-assessment 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.

OUTCOME OF VOLUNTARY SELF-ASSESSMENT

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
