
ISPS Code

Notice to ship owners, managers, Masters, Approved Nautical Inspectors, Recognised Organisations and surveyors

(This Notice supersedes BMA Information Bulletin No.70)

1. Purpose

- 1.1. This Notice provides instructions on maritime security for Bahamian ships.
- 1.2. This Notice is to be read in conjunction with IMO Maritime Safety Committee Circulars MSC/Circ.1072, MSC/Circ.1074, MSC/Circ.1097, MSC/Circ.1111, MSC/Circ.1132, MSC/Circ.1156, MSC.1/Circ.1189, MSC.1/Circ.1191, MSC.1/Circ.1194, MSC.1/Circ.1217, MSC.1/Circ.1305, MSC.1/Circ.1342, MSC.1/Circ.1390 and MSC-MEPC.2/Circ.9.

2. Application

- 2.1. This Notice applies to the types of ships specified in Regulation 2.1.2 of Chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974, as amended (SOLAS Chapter XI-2), namely:
- i. Passenger ships, including High Speed Passenger Craft,
 - ii. Cargo ships of 500 gross tonnage and above, including High Speed Craft, and
 - iii. Mobile Offshore Drilling Units (MODUs).
- 2.2. The Bahamas Maritime Authority (BMA) requires that the ship types to which this Notice applies are continuously certificated by a Bahamas approved Recognised Security Organisation (RSO) as compliant with the International Ship and Port Facility Security Code (ISPS Code), even if they are not engaged on international voyages¹.
- 2.3. Registration of ships with The Bahamas is based upon them being engaged in foreign going trade, i.e. operating outside the territorial waters of The Bahamas. As such, the BMA applies international standards to such ships irrespective of whether the affected voyages are international or solely between ports within the territorial waters of a single country outside The Bahamas.

¹ An international voyage is a voyage from a port in one country to a port in another country (Merchant Shipping Act (Ch.246), s.2).

- 2.4. Ships to which SOLAS Chapter XI-2 and the ISPS Code do not apply but which operate in ports or interact with ships subject to the requirements of the Convention and Code are strongly encouraged to obtain a voluntary “Certificate of Compliance” from a Bahamas approved RSO.
- 2.5. It should be noted that both SOLAS Chapter XI-2 and part A of the ISPS Code have no provision for the granting of exemptions.

3. Mandatory requirements

- 3.1. The provisions of Part B of the ISPS Code, which includes specific and prescriptive requirements, are non-mandatory but should be taken into account.
- 3.2. Mandatory requirements are outlined in:
 - i. SOLAS Chapter XI-2, as amended;
 - ii. The Ship and Port Facility (Security) Regulations, 2016, as amended;
 - iii. Part A of the ISPS Code, as amended.

4. Communication of general security information

- 4.1. Routine security issues, enquiries, or reports of difficulties encountered during Port State Control inspections, may be directed to the BMA Inspection and Surveys Department (tech@bahamasmartime.com), but not through the emergency telephone number.
- 4.2. The BMA Emergency Response telephone number is only to be used in the case of a genuine maritime security emergency requiring intervention from the Administration, i.e. hijack, terrorist attack, piracy, any incident involving the use of firearms, any bomb threat, any use or threat of use of force.

5. Recognised Security Organisations (RSOs)

- 5.1. The Bahamas has formally approved a number of organisations to undertake the approval of Ship Security Plans (SSP) and the verification and certification of ships for compliance with SOLAS XI-2 and the ISPS Code, as listed in BMA Marine Notice MN002.
- 5.2. An RSO which has been involved in the preparation of an SSP is not permitted to engage in the statutory approval and certification of that plan.

- 5.3. Queries relating to RSOs for port facilities in The Bahamas are not the responsibility of the BMA and should be referred to the Bahamas Port Department (portcustomerservice@bahamas.gov.bs).

6. Documentation and records

- 6.1. The applicable provisions of Part B of the ISPS Code should be used in the development of the SSP. The SSP, along with the Ship Security Assessment, is to be submitted to the RSO during the initial certification process.
- 6.2. A copy of the SSP is not required to be submitted to the BMA.
- 6.3. Changes and amendments to the SSP are required to be submitted to the RSO for review although such changes must be fundamental to the plan. For example, purchase of equipment that performs the same as its predecessor would not require approval; however installation of new equipment that changes/enhances the efficacy of the plan would need to be approved. Similarly, changes of crew personnel, on a like for like basis, would not need approval but changes to the crew complement, where there is an impact on the security plan, would need to be approved.
- 6.4. The SSP and the records of activities addressed in the SSP shall be in the working language(s) of the ship. If that working language is not English then a translation into English shall be provided and maintained.
- 6.5. The SSP must outline the function of the listed equipment and identify the measures to be introduced in the event of failure.
- 6.6. Records of activities provided for by the SSP, including Declarations of Security and the record of the ship Security Level, shall be maintained onboard for a period covering at least the previous ten (10) calls at port facilities.
- 6.7. During and after the period specified in 6.6 above, records shall be maintained ashore by the Company² in accordance with its own procedures for record keeping. The Company shall note that if any activity is referred to in the Official Log Book (OLB), that record shall be retained as an attachment to the OLB and consequentially the record is required to be maintained for a period of seven (7) years.
- 6.8. Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation must be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or the ship.

² The "Company" is the entity responsible for the management of the ship in accordance with the ISM Code. For ships which the ISM Code is not applicable, Company is the Managing Owner in accordance with Section 52 of the Merchant Shipping Act.

- 6.9. The plan may be kept in an electronic format. In such a case, it shall be protected by means to prevent it from being deleted, destroyed or overwritten.
- 6.10. The plan must be protected from unauthorized access or disclosure.
- 6.11. Ship Security Plans are not generally subject to inspection by officers of a port state. However, if there are clear grounds for believing that the ship is in violation of the requirements of Chapter XI-2 of SOLAS or of the ISPS Code, limited access to the specific sections of the plan relating to the non-compliance is allowed, but only with the consent of the BMA or the master of, the ship.

7. Company Security Officer (CSO), Ship Security Officer (SSO) and seafarers with designated security duties and security related training and instructions

- 7.1. The Company is responsible for notifying the BMA of the designated CSO for every Bahamian registered ship under its control. For all newly registered ships, the CSO's full contact details shall be included on the form R104. The same applies if the Company changes or the identity of the ship changes.
- 7.2. Changes to the CSO contact details only may be provided to the BMA as an email notification to tech@bahamasmaritime.com.
- 7.3. The BMA will provide acknowledgement letters confirming the appointment of the CSO by email.
- 7.4. Certification for Ship Security Officers (SSO) and relevant security training and instruction for seafarers is dealt with in BMA Information Bulletin No.118.
- 7.5. The BMA does not specify any required rank for the SSO. It is however expected that this role will be filled by the Master or a senior officer, having received training as an SSO.

8. BMA security communications including Ship Security Alert System (SSAS)

- 8.1. The BMA will use the existing Marine Notice/Information Notice/Technical Alert system to inform interested parties of any changes to the security level applicable to Bahamian registered ships. The current security level is available on the home page of the BMA website (www.bahamasmaritime.com) or by contacting the BMA Inspections and Surveys Department. The BMA does not require that the CSO acknowledges

receipt of a change of security level by The Bahamas but the CSO must maintain a log of the current security level, and any changes.

- 8.2. Where the security level is changed by The Bahamas, or the contracting Government of the port in which a Bahamas registered ship is operating, the SSO is required to send an acknowledgement to the Company. The SSO or CSO shall notify the BMA on any changes to the onboard security level by sending an email notification to tech@bahamasmaritime.com without delay. The BMA will acknowledge these communications and advise the Bahamas ISPS Compliance Unit accordingly.
- 8.3. The BMA requires notification of a major security threat or incident without delay³. This includes any Ship Security Alert (SSA), **once verified as authentic by the CSO**. This notification is to be made to the Emergency Response Officer on the BMA emergency telephone number **+44 20 3922 2619**. The notifying party must have available at least the following information:
- Ships details: Name, Official number, IMO number;
 - Geographical location of ship;
 - Cargo, if any;
 - Number of persons on board.

9. Programming of Ship Security Alert System (SSAS)

- 9.1. The BMA **is not** to be designated as the receiving authority for SSAS alerts. The SSAS must be programmed to ensure that the security alert is sent to the Competent Authority, i.e. the Company or other recipient designated by the Company, and not to any other party, in accordance with Regulation 6 of SOLAS Chapter XI-2.
- 9.2. CSOs are required to verify that the SSAS onboard their Bahamian registered ships have been correctly programmed, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised.

10. Bahamas procedure for drills and testing of ship's security measures

- 10.1. The BMA accepts that a safety drill, which has a security component within it, can be credited as a security drill. The interval between security drills shall not exceed three (3) months. The Bahamas does not require notification of security drills.
- 10.2. In addition, and in cases where more than 25 % of the ship's personnel have been changed with personnel that have not previously participated in any security drill on

³ A major security incident or threat is defined as a hijack, terrorist attack, piracy, any incident involving the use of firearms, any bomb threat, any use or threat of use of force.

that ship within the last three (3) months, a security drill shall be conducted within one week of such a change.

- 10.3. The Company shall conduct an annual security exercise with one or more ships within its fleet, which may include participation of the CSO, Port Facility Security Officers (PFSO), relevant authorities of contracting Governments as well as SSOs, if available. These exercises may be full scale or live; table top simulation or seminar or combined with other exercises held, such as search and rescue or emergency response.
- 10.4. The results of exercises and any lessons learnt should be formulated into a report and circulated to the Company's fleet.
- 10.5. If, during a company security exercise, a CSO wishes to verify the emergency communication route between the Company and BMA, the CSO shall notify the BMA by email at least one working day in advance of the exercise commencing. The BMA may issue specific instructions on receipt of such a notification.
- 10.6. The Bahamas does not require notification of testing of the SSAS. However, in accordance with the provisions of the Code, The Bahamas may test the preparedness of Bahamian ships by the use of a test simulation or communication. In such cases the word "TEST" will be clearly noted in any transmissions.
- 10.7. All visitors to the ship shall be challenged by the person on gangway duty watch to provide identification and to state their business. They shall remain accompanied on board at all times. BMA Approved Nautical Inspectors are issued with photograph identity cards which must be presented on entry to the ship. In case of doubt a CSO or SSO may contact the BMA Inspection and Surveys Department for verification of the inspector's identity.

11. Bahamian ships entering ports operating at a higher security level than that set by The Bahamas

- 11.1. The ISPS Code places the responsibility for setting security levels for ships with the relevant Flag State, but a Port State may also require a ship to raise its security level for the duration of its stay within a port or at a particular port facility.
- 11.2. Bahamian ships must operate at a security level the same as, or higher than, that advised by the port facility whilst at that facility.
- 11.3. If a Bahamian ship is operating at a higher level, as set by the Bahamas, than that set by the port's Contracting Government, arrangements are to be agreed with the Port Facility Security Officer (PFSO) to allow the ship to continue to operate at the security level set by The Bahamas.

- 11.4. Coastal States may advise ships that the security situation in their territorial waters requires heightened security and it is for the ship to determine what measures to take in response to such information.
- 11.5. Ships are permitted to implement additional security measures for the duration of the stay at a particular port facility in cases where heightened security is believed to be necessary. This may also apply to port facilities which are not ISPS compliant.
- 11.6. Any change of security level to one that is higher than that set by the Bahamas, or implementation of security measures equivalent to a higher security level than that set by the Bahamas, is to be advised by email to tech@bahamasmaritime.com. The BMA will acknowledge these communications and advise the Bahamas ISPS Compliance Unit accordingly.
- 11.7. Any change of security level to Level 3, or implementation of security measures equivalent to Level 3, is to be notified to the BMA Emergency Response Officer at the first available opportunity on the emergency telephone number **+44 20 3922 2619**.

12. Bahamian ships entering ports which are not compliant with the ISPS Code

- 12.1. The SSO or Master shall request that a Declaration of Security be completed by the Port Facility Security Officer (PFSO) or port facility management. If this request is refused then the ship shall use the Declaration of Security to record the security measures and the Declaration of Security shall be completed and signed by the Master, or the SSO if the ship has a designated SSO who is not the Master. The completed Declaration of Security shall be retained as per paragraph 6.6 above.
- 12.2. The ship shall implement additional security measures to the extent that the CSO and/or SSO and/or Master deem necessary. It may be noted that this does not necessarily mean that all the measures specified in the SSP for the next security level must be implemented.
- 12.3. Any change of security level to one that is higher than that set by the Bahamas, or implementation of security measures equivalent to a higher security level than that set by the Bahamas, is to be advised by email to tech@bahamasmaritime.com. The BMA will acknowledge these communications and advise the Bahamas ISPS Compliance Unit accordingly.
- 12.4. Any change of security level to Level 3, or implementation of security measures equivalent to Level 3, is to be notified to the BMA Emergency Response Officer at the first available opportunity on the emergency telephone number **+44 20 3922 2619**.

13. Self-propelled & non-self-propelled offshore floating units

- 13.1. In accordance with MSC-MEPC.2/Circ.9, FPSO/FSO/FSU and similar units should, in order to facilitate interaction with other ships, comply with SOLAS Chapter XI-2 and the ISPS Code as applicable.
- 13.2. All offshore floating units including Single Buoy Moorings (SBMs) which interface with ships and port facilities covered by the ISPS Code shall contact the Designated Authority of the coastal State, in whose sea they operate, and ascertain their status with respect to their local designation under the ISPS Code and the security arrangement required by that designation. The Bahamas is aware that self-propelled and non-self-propelled offshore floating units may be considered as port facilities by the coastal State in whose sea they are operating.
- 13.3. The BMA recommends that Companies operating affected units carry out a ship security assessment, taking into consideration the guidance contained in Part B of the ISPS Code, and develop a ship security plan. The plan should be submitted to a Bahamas RSO for approval. After a visit to the unit to verify the effectiveness of the plan and its implementation, the RSO will issue a Statement of Compliance attesting to the effectiveness of the plan in seeking the detection and deterrence of acts which threaten maritime security. The unit is to be subjected to re-verification to confirm the satisfactory condition of the security system between the second and third anniversary date of the Statement of Compliance.
- 13.4. Self-propelled and non-self-propelled offshore floating units may undertake interim voyages from their operational area but the Company should note that the commercial operation of such units may be affected by the lack of certified onboard security procedures.

14. Verification and Certification for Ships

- 14.1. The certification process relevant to an International Ship Security Certificate (ISSC) for a ship will normally involve the following steps:
- i. interim verification;
 - ii. initial verification;
 - iii. intermediate verification;
 - iv. renewal verification; and, if necessary
 - v. additional verification.

14.2. **Interim Verification**

14.2.1. An Interim ISSC may be issued:

- to new ships on delivery;
- when a Company takes on responsibility for the operation of a ship which is new to the Company; or
- when a ship changes flag.

14.2.2. Interim ISSCs are issued for a period not exceeding 6 months. The BMA may, in special cases, extend the validity of an Interim ISSC for a further period which shall not exceed 6 months from the date of expiry. When an interim ISSC is extended, the full-term ISSC should be dated from the date of completion of the initial verification.

14.3. **Initial Verification**

14.3.1. an initial verification shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of SOLAS Chapter XI-2, the ISPS Code, and the approved Ship Security Plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of SOLAS Chapter XI-2 and the ISPS Code, is in satisfactory condition and fit for the service for which the ship is intended.

14.3.2. On satisfactory completion of the assessment of the ships, they shall be issued with a full-term ISSC.

14.3.3. During an initial verification audit, if it is found that the ship does not merit the issuance of a full term certificate due to the number of non-conformities, a short term ISSC valid for 3 months is to be issued so that another audit can be carried out prior to the issuance of a full term certificate. This is to be done in consultation with the BMA.

14.3.4. The RSO should send copies of all certificates to the BMA unless they are available to the BMA on the RSO's online database.

14.4. **Intermediate Verification**

14.4.1. The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate.

14.4.2. If only one intermediate verification is to be carried out, it should take place between the second and third anniversary date of the issue of the ISSC.

14.4.3. It should be noted that there is no provision in the ISPS Code to extend the window for the intermediate verification and if the intermediate audit is not carried out within the window, the ISSC becomes invalid as per ISPS Code A19.3.8. In such cases a renewal verification will be required, with the extent of audit at least that of an intermediate verification. A new ISSC may be issued on completion of the renewal survey, which shall have an expiry date not later than the expiry date of the original certificate.

14.5. ***Renewal Verification***

14.5.1. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of SOLAS Chapter XI-2, the ISPS Code; and the approved SSP; and is in satisfactory condition and fit for the service for which the ship is intended.

14.5.2. Renewal verification may be carried out within three months before the date of expiry of the ISSC and should be completed before the date of expiry.

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

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

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

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

14.6. ***Additional Verification***

14.6.1. Additional ISSC audits may be required by the BMA in specific circumstances, e.g. following adverse Port State Control inspections/detentions, Bahamas safety inspections, IACS PR17 reports, etc., or in the case of reactivation after the interruption

of operations due to a period out of service, or in order to verify that effective corrective actions have been taken and/or are being properly implemented.

- 14.6.2. Where ships are detained under the Port State Control regime, the PSC authority may require an additional audit before the ship is released from detention.
- 14.6.3. On satisfactory completion of the shipboard assessment, the ISSC should be endorsed with the additional verification.
- 14.7. A copy of the certificate and a copy of the verification report must be transmitted as soon as possible to the BMA.
- 14.8. ***ISSC Validity period and extensions***
- 14.8.1. An ISSC shall be issued for a period which shall not exceed five years.
- 14.8.2. If a certificate is issued for a period of less than five years, the BMA may agree to extend the validity of the certificate beyond the expiry date to a maximum of five years upon receiving an application through the RSO, provided that the verifications for a certificate issued for a period of five years are carried out as appropriate.
- 14.8.3. If a ship at the time when a certificate expires is not in a port in which it is to be verified, the BMA may extend the period of validity of the certificate upon receiving an application through RSO, but this extension will be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is verified, and then only in cases where it appears proper and reasonable to do so. No certificate will be extended for a period longer than three months, and the ship to which an extension is granted may not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate. When the renewal verification is completed, the new certificate will be valid to a date not exceeding five years from the expiry date of the existing certificate before the extension was granted.
- 14.8.4. A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the RSO for a period of grace of up to one month from the date of expiry stated on it upon receiving the BMA's concurrence. When the renewal verification is completed, the new certificate will be valid to a date not exceeding five years from the date of expiry of the existing certificate before the extension was granted.

15. Queries

- 15.1. Any queries on this Notice may be addressed to tech@bahamasmaritime.com or any BMA office.

