The Bahamas Maritime Authority

Version No. 1.3
Issue Date 19/11/2026
Effective Date 19/11/2026

ISPS Code

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

1. Purpose

1.1. This Notice provides instructions on the application of maritime security requirements to Bahamian ships and other units addressed by this Notice.

1.2. This Notice should be read in conjunction with relevant International Maritime Organization (IMO) maritime security guidance, including the instruments listed in the Annex to this Notice.

2. Application

2.1. This Notice applies to the types of ships specified in Regulation 2.1.1 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 ships of the types specified in paragraph 2.1 to comply with SOLAS Chapter XI-2 and the International Code for the Security of Ships and of Port Facilities (ISPS Code) and to be continuously certificated by a Bahamas approved Recognised Security Organisation (RSO), irrespective of whether they are engaged on international voyages[1].

2.3. The BMA applies the requirements of SOLAS Chapter XI-2 and the ISPS Code to ships specified in paragraph 2.1 irrespective of whether an individual voyage is an international voyage or is solely between ports within the territory of another State.

2.4. Ships to which SOLAS Chapter XI-2 and the ISPS Code do not apply, but which operate in ports or interface with ships subject to those requirements, are strongly encouraged to obtain a voluntary "Certificate of Compliance" from a Bahamas approved RSO.

[1] An international voyage is a voyage from a port in one country to a port in another country (section 2, Merchant Shipping Act, 2021).

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. Part B of the ISPS Code provides guidance regarding the provisions of SOLAS Chapter XI-2 and Part A of the ISPS Code and shall be taken into account where applicable. Companies[2] and ships shall also comply with any provisions of Part B which are made mandatory through SOLAS Chapter XI-2.

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 enquiries, reports and matters arising from Port State Control inspections may be directed to the BMA Inspection and Surveys Department (tech@bahamasmaritime.com). The BMA emergency telephone number shall not be used for routine matters.

4.2. The BMA emergency telephone number is only to be used for a maritime security emergency requiring intervention by the Administration, as described in paragraph 8.3.

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 Chapter XI-2 and the ISPS Code, as listed in BMA Marine Notice MN002.

5.2. An RSO shall not approve an SSP where the RSO has undertaken the Ship Security Assessment or prepared the SSP for that ship.

[2] The 'Company' is the entity responsible for the operation and management of the ship in accordance with the ISM Code (SOLAS Chapter IX), as applied under the Merchant Shipping Act, 2021. Where the ISM Code is not applicable, the Company is the entity recorded as responsible for the operation of the ship in accordance with regulation 5(3)(d) of the Merchant Shipping (Registration) Regulations, 2026.

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 relevant guidance in Part B of the ISPS Code shall be taken into account 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. Amendments to the SSP which affect the scope or effectiveness of the approved security arrangements shall be submitted to the RSO for approval before implementation. Changes which do not affect the approved security arrangements, such as replacement of equipment on a like-for-like basis or routine changes of personnel which do not affect responsibilities identified in the SSP, need not be submitted for approval.

6.4. The SSP and the records of activities addressed in the SSP shall be in the working language(s) of the ship. Where the working language is not English, an English translation 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. The records required by section 10 of Part A of the ISPS Code, including Declarations of Security and the records of changes in security level, shall be retained on board. The BMA requires these records to cover at least the previous 10 calls at port facilities.

6.7. Thereafter, records shall be maintained ashore by the Company in accordance with its record-keeping procedures. Where a record forms part of, or is retained as an attachment to, 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.

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 duly authorised by a Contracting Government to carry out control and compliance measures, including Port State Control. Where there are clear grounds for believing that the ship is not in compliance with SOLAS Chapter XI-2 or Part A of the ISPS Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the SSP, limited access to the specific sections of the SSP relating to the non-compliance is exceptionally allowed with the consent of the BMA or the master. **However, the provisions of the SSP relating to sections A/9.4.2, A/9.4.4, A/9.4.5, A/9.4.7, A/9.4.15, A/9.4.17 and A/9.4.18 of the ISPS Code are considered confidential and shall only be accessed with the consent of the BMA.**

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 shall notify the BMA of the designated CSO for each Bahamian ship under its management. For a newly registered ship, the CSO's full contact details shall be provided on Form R104.

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 Marine Notice 27.

7.5. The BMA does not prescribe a minimum rank for the SSO. The person designated as SSO shall meet the applicable training and certification requirements and have sufficient authority to perform the functions and responsibilities specified in the ISPS Code.

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

8.1. The BMA will use Marine Notices, Information Notices or Technical Alerts, as appropriate, to advise interested parties of any changes to the security level applicable to Bahamian 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 of 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 delay[3]. 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 3869 8748**. The notifying party must have available at least the following information:

- Ship details: name, official number, IMO number;
- Geographical location of ship;
- Cargo, if any;
- Number of persons on board.

8.4. 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.

8.5. 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 3869 8748**.

9. Programming of Ship Security Alert System (SSAS)

9.1. The BMA **shall not** be designated as the direct recipient of SSAS alerts. The SSAS shall be programmed to transmit the alert to the Company or another recipient designated by the Company in accordance with Regulation 6 of SOLAS Chapter XI-2.

9.2. CSOs are required to verify that the SSAS on board 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.

[3] A major security threat or incident 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.

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

10.1. Security drills shall be conducted at least once every three months. A drill conducted for another purpose may also satisfy this requirement where it adequately tests relevant security duties and procedures.

10.2. Where more than 25% of the ship's personnel have been changed at any one time by personnel who have not previously participated in a security drill on that ship within the preceding three months, a security drill shall be conducted within one week of the change.

10.3. Security exercises shall be carried out at least once each calendar year, with no more than 18 months between exercises. Exercises should test communications, coordination, resource availability and response and may include participation by CSOs, relevant authorities of Contracting Governments, Port Facility Security Officers (PFSOs) and SSOs. These exercises may be full scale or live exercises, tabletop simulations or seminars, and may be combined with other exercises, such as search and rescue or emergency response exercises.

10.4. The results of exercises and any lessons learned 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. Access to the ship shall be controlled in accordance with the approved SSP and the applicable measures at the prevailing security level.

10.8. BMA Inspectors are issued with photographic identification, which shall be presented when boarding the ship. In case of doubt, the CSO, SSO or master may contact the BMA Inspection and Surveys Department to verify an 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. Where a Bahamian ship is operating at a security level set by the Bahamas which is higher than that applying at the port facility, the ship shall liaise with the PFSO to coordinate the appropriate security measures and procedures.

11.4. Coastal States may advise ships that the security situation in their territorial waters requires heightened security. 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.

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 in accordance with paragraph 6.6.

12.2. The ship shall implement additional security measures to the extent that the CSO, SSO and Master, as appropriate, 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.

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

13.1. In accordance with MSC-MEPC.2/Circ.9, floating production, storage and offloading units (FPSOs), floating storage and offloading units (FSOs), floating storage units (FSUs) 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 verification to confirm the satisfactory condition of the security system between the second and third anniversary dates 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 six months, in accordance with section A/19.4.4 of the ISPS Code. The BMA may, in exceptional circumstances, permit

the issue of a second, consecutive Interim ISSC provided that the purpose of the request for a second Interim ISSC is not, in the BMA's opinion, to avoid full compliance with SOLAS Chapter XI-2 and Part A of the ISPS Code. When a second consecutive Interim ISSC is issued, it shall be for a period not exceeding six months from the date of expiry of the original interim ISSC. When the full-term ISSC is issued, it 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 the ship's 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 comply with the applicable requirements of SOLAS Chapter XI-2 and the ISPS Code, are in satisfactory condition and are fit for the service for which the ship is intended.

14.3.2. On satisfactory completion of the verification of the ship, it shall be issued with a full-term ISSC.

14.3.3. 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 dates of the issue of the ISSC.

14.4.3. There is no provision in the ISPS Code to extend the window for the intermediate verification. If the intermediate verification is not carried out within the required window, the ISSC becomes invalid in accordance with section A/19.3.8 of the ISPS Code. In such cases, a renewal verification will be required. A new ISSC may be issued on completion of the renewal verification, with an expiry date no 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 comply with the applicable requirements of SOLAS Chapter XI-2, the ISPS Code and the approved SSP and are 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 verifications may be required by the BMA in specific circumstances, including following adverse Port State Control inspections or detentions, Bahamas inspections or IACS PR17 reports; following reactivation after a period out of service; or to verify that effective corrective actions have been taken and are being properly implemented.

14.6.2. Following a Port State Control (PSC) detention involving security-related deficiencies, an additional verification may be required by the BMA or requested by the PSC authority, as applicable, 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.

14.6.4. A copy of the certificate and verification report shall be sent to the BMA as soon as possible.

14.7. ***ISSC validity period and extensions***

14.7.1. An ISSC shall be issued for a period which shall not exceed five years.

14.7.2. 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.

14.7.3. 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 the 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.

14.7.4. 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.

Annex – IMO maritime security guidance

1. The following International Maritime Organization (IMO) guidance should be taken into account, as applicable:

i. **MSC/Circ.1072** *Guidance on provision of ship security alert systems*;
ii. **MSC/Circ.1073** *Measures to enhance maritime security*;
iii. **MSC/Circ.1074** *Measures to enhance maritime security*;
iv. **MSC/Circ.1097** *Guidance relating to the implementation of SOLAS Chapter XI-2 and the ISPS Code*;
v. **MSC/Circ.1104** *Implementation of SOLAS Chapter XI-2 and the ISPS Code*;
vi. **MSC/Circ.1111** *Guidance relating to the implementation of SOLAS Chapter XI-2 and the ISPS Code*;
vii. **MSC/Circ.1132** *Guidance relating to the implementation of SOLAS Chapter XI-2 and the ISPS Code*;
viii. **MSC/Circ.1156** *Guidance on the access of public authorities, emergency response services and pilots on board ships to which SOLAS Chapter XI-2 and the ISPS Code apply*;
ix. **MSC.1/Circ.1189** *Interim scheme for the compliance of special purpose ships with the special measures to enhance maritime security*;
x. **MSC.1/Circ.1190** *Guidance on the provision of information for identifying ships when transmitting ship security alerts*;
xi. **MSC.1/Circ.1191** *Further reminder of the obligation to notify flag States when exercising control and compliance measures*;
xii. **MSC.1/Circ.1194** *Effective implementation of SOLAS Chapter XI-2 and the ISPS Code*;
xiii. **MSC.1/Circ.1217** *Interim guidance on voluntary self-assessment by Companies and Company Security Officers (CSOs) for ship security*;
xiv. **MSC.1/Circ.1235** *Guidelines on security-related training and familiarization for shipboard personnel*;
xv. **MSC.1/Circ.1305** *Revised guidance to Masters, Companies and duly authorized officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port*;
xvi. **MSC.1/Circ.1342** *Reminder in connection with shore leave and access to ships*; and
xvii. **MSC-MEPC.2/Circ.9** *Guidance for the application of safety, security and environmental protection provisions to FPSOs and FSUs*.

Revision History

Version	Description of Revision
1.0	First Issue
1.1	Updated ERO phone number
1.2	Updated Interim verification section (paragraph 14.2.2)
1.3	Updated regulatory references and maritime security requirements; revised Ship Security Plan approval and access provisions, security communications, drills and exercises, and verification and certification requirements; added Annex of relevant IMO maritime security guidance; and editorial amendments.