Bulletin 030 – ISPS Code

Barbados Maritime Ship Registry

Revision No:	1.0	Issue Date:	20 Aug 2025	Effective Date:	20 Aug 2025

Notice to: Shipowners, Operators, Officers, Flag State Inspectors and Recognised Organisations.

1. References

a) Barbados Merchant Shipping Act, 2024
b) The International Ship and Port Facility Security Code (ISPS Code)
c) International Convention for the Safety of Life at Sea (SOLAS)
d) Bulletin 035 – Piracy and Armed Robbery
e) PPR01-F04 Security Communication Statement
f) The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)
g) Bulletin 021 – BMSR Certificates of Endorsements
h) IMO MSC/Circ.1154 Guide Training & Certification Security Officers
i) Bulletin 008 – Permits Exemptions and Equivalences

2. Purpose

2.1 This Bulletin provides consolidated guidance on maritime security in accordance with the ISPS Code. It establishes the standards and procedures set out by the Barbados Maritime Ship Registry (BMSR), covering requirements for vessels under the Barbados flag and encouraging harmonised application for maximum security and regulatory alignment.

2.2 Full compliance with ISPS Code Part A and SOLAS Chapter XI-2 is required.

2.3 ISPS Code Part B, which provides guidance on meeting Part A's requirement is recommendatory, though it may be mandatory in some coastal states.

3. Application

3.1 This Bulletin applies to:

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

.2 Cargo ships, including high-speed craft and commercial yachts of 500 gross tonnage (GT) and above;

.3 Special Purpose Ships of 500 GT and above;

.4 Self-propelled Mobile Offshore Drilling Units (MODUs) capable of international voyages.

3.2 The ISPS Code and this Bulletin does not apply to:

.1 Cargo ships and commercial yachts under 500 GT;

.2 Offshore Support Vessels;

.3 Pleasure/Private yachts;

.4 Non-self-propelled barges and MODUs or location-bound offshore units (FPSOs/FSUs).

3.3 Vessels not subject to mandatory compliance with the ISPS Code as per Sec. 3.2 above may do so voluntarily. Evidence of voluntary compliance is to be verified and certified by a Barbados Recognised Security Organisation (RSO).

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 BMSR Ops@barbadosmaritime.com , but not through the emergency telephone number.

4.2 The BMSR Emergency Response telephone number is only to be used in the case of a genuine maritime security emergency requiring intervention from the BMSR such as hijack, terrorist attack, piracy, any incident involving the use of firearms, any bomb threat, any use or threat of use of force.

5. Company Security Officer (CSO) and Ship Security Officer (SSO)

5.1 The Company shall appoint a Company Security Officer (CSO) for each of its vessels, who shall be an internal employee of the Company and shall assume all duties and responsibilities required by the ISPS Code, Part A, Sec. 11, for one or more of its vessels.

5.2 The Company shall notify the BMSR of the designated CSO for every Barbados vessel under its control. For all newly registered vessels, the CSO's full contact details and the list of vessels shall be included on the form PPR01-F04 Security Communication Statement. The same applies if the Company changes or the identity of the vessel changes.

5.3 Changes to the CSO contact details only may be provided to the BMSR as an email notification to registry@barbadosmaritime.com.

5.4 The BMSR will provide acknowledgement letters confirming the appointment of the CSO by email.

5.5 Companies shall ensure that CSOs are trained as required by the ISPS Code, Part A, Sec. 13 and demonstrate the competencies in line with the requirements set in the Annex of MSC/Circ.1154 and IMO Model Course 3.20.

5.6 A Ship Security Officer (SSO) shall be designated on each vessel and shall carry out or perform all duties and responsibilities required by the ISPS Code, Part A, Sec. 12.

5.7 The SSO shall be either the Master or a senior officer, who shall have a certificate of proficiency in compliance with STCW Reg. VI/5, and a BMSR Certificate of Endorsement (COE) issued by the BMSR as per Sec. 4 of Bulletin 021.

6. Ship Security Plan (SSP)

6.1 Each vessel shall carry on board a specific Ship Security Plan (SSP) approved by a Barbados RSO in compliance with the ISPS Code, Part A, Sec. 9. Subsequent amendments to the SSP that are related to the requirements of ISPS CodeISPS Code, Part A, from Sec. 9.4.1 to 9.4.18, shall also be reviewed and approved.

6.2 The SSP must remain strictly confidential, and access should only be permitted to the Barbados RSO auditors.

6.3 The SSP shall outline equipment functions, response to equipment failure, and protection measures, and shall address:

.1 Unlawful acts threatening the safety of the vessel and the security of its passengers and crew, based on a security risk assessment;

.2 Countermeasures to protect against terrorism, piracy, stowaways, smuggling and armed robbery when operating in high-risk areas. See Bulletin 035 for more information;

.3 The Master's overriding authority to make decisions relating to vessel safety and security.

6.4 The implementation of the SSP, including amendments, must be verified by a Barbadian RSO during an onboard attendance.

6.5 There is no need to send a copy of the SSP to the BMSR, but BMSR reserve the right to ask for the SSP at any time if this is deemed necessary.

6.6 SSP are not generally subject to inspection by Port State Control officers. However, if there are clear grounds for believing that the vessel is in violation of the requirements of SOLAS Chapter XI-2 or of the ISPS Code, limited access to the specific sections of the SSP relating to the non-compliance is allowed, but only with the consent of the BMSR or the Master of the vessel.

6.7 The SSP and the records of activities addressed in the SSP shall be in the working language(s) of the vessel. If that working language is not English, then a translation into English shall be provided and maintained.

6.8 Records of activities provided for by the SSP, including Declarations of Security and the record of the vessel security Level, shall be maintained onboard for a period covering at least the previous ten (10) calls at port facilities.

6.9 During and after the period specified in Sec. 6.8 above, records shall be maintained ashore by the Company in accordance with its own procedures for record keeping. The Company shall note that if any activity is referred to in the vessel Official Logbook (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.

6.10 The SSP may be kept in electronic format. In such a case, it shall be protected by means to prevent it from being deleted, destroyed, or overwritten and from unauthorised access or disclosure.

6.11 The SSO shall review the SSA and the SSP in conjunction with an on-scene security survey at intervals not exceeding 12 months. The SSP shall be amended if inadequacies are identified during this annual review. Additional vessel security risks may also be identified during trainings, exercises, drills, or following a security incident.

7. Vessel Security Levels

7.1 A vessel shall operate at the security level established by the BMSR, see Sec. 8 below, or port facility, which is typically based on the level set by the port State.

7.2 If a security level has not been set by the port State, there still may be a need for enhanced security measures due to reported threats in the area.

7.3 Security measures equivalent to a higher security level may be implemented if a vessel deems it necessary to operate at a higher security level than the port.

7.4 The security levels shall be set as per ISPS Code, Part A, Sec. 13.1:

.1 **Level 1 – Normal**, which means the level for which minimum appropriate protective security measures shall be maintained at all times.

.2 **Level 2 – Heightened**, means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

.3 **Level 3 – Exceptional**, which means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

7.5 The SSO or CSO shall notify the BMSR on any changes to the onboard security level by sending an email notification to ops@barbadosmaritime.com without delay. The BMSR will acknowledge these communications and advise accordingly.

8. Barbados Security Level

8.1 The current security level for Barbadian vessel is set to **Level 1 – Normal.**

8.2 The BMSR shall issue a Marine Circular "Barbados Security Level Update" to inform interested parties of any changes to the above security level.

9. Communication of Major Security Threat

9.1 The BMSR requires notification of a major security threat or incident without delay. This includes any Ship Security Alert (SSA), once verified as authentic by the CSO.

9.2 The notification is to be made to the BMSR Emergency Response Officer (ERO) on the BMSR emergency ONLY telephone number **+44 (0)7494116754** and with a following email to ops@barbadosmaritime.com with at least the information below:

.1 Vessel Name and IMO number;

.2 Geographical location of vessel;

.3 Security threat description;

.4 Number of people on board;

.5 Cargo, if any;

.6 Local authorities informed, if any;

.7 Actions taken;

10. Ship Security Alert System (SSAS)

10.1 The BMSR shall not be designated as the receiving authority for SSAS alerts.

10.2 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 SOLAS Chapter XI-2 Reg. 6.

10.3 The CSO shall remain a recipient of all SSAS transmissions along with Company designated Competent Authority.

10.4 Companies are required to designate either an internal appointee (preferably the CSO or Alternate Company Security Officer (ACSO) or an external, qualified third party to serve as the "Competent Authority" to receive all SSAS alerts and take appropriate action.

10.5 BMSR requires that to be considered qualified, a Competent Authority shall:

.1 Be available at all times (on a 24/7 basis) to receive and act upon SSAS alerts;

.2 Be able to accurately identify and react to real, test, or false alerts;

.3 Understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code and this Bulletin;

.4 Maintain a current contact list of relevant authorities (BMSR, Maritime Rescue Coordination Centres (MRCCs), Coastal State Authorities, Information Sharing Centres) to be used in the event of an actual alert; and

.5 Participate in drills or exercises involving tests of the SSAS.

.6 The Competent Authority is to acknowledge and respond to all test messages directly, ensuring the proper functioning of SSAS equipment and verifying the accuracy of the transmitted data without the need for acknowledgement of receipt by the BMSR.

10.6 Third party Competent Authorities are not to contact the BMSR directly. All direct communication with BMSR must only be from the Company. Where a third party is appointed as Competent Authority, the third party is to inform the company and in turn company is responsible to notify the BMSR immediately for cases of real Major Security Threat as per Sec. 9 above.

10.7 SSAS alert messages shall include at the least the following information:

.1 Vessel Name;

.2 IMO Number;

.3 Call Sign;

.4 Maritime Mobile Service Identity (MMSI) Number;

.5 Date and Time (UTC);

.6 Global Navigation Satellite System (GNSS) position (latitude and longitude);

.7 Course and Speed;

.8 CSO 24/7 phone number; and

.9 Alternate CSO 24/7 phone number.

11. Procedures for Drills and Exercises

11.1 The BMSR accepts that a vessel safety drill, which has a security component within it, can be credited as a security drill. The interval between vessel security drills shall not exceed three (3) months.

11.2 In addition to the drill as mentioned in Sec. 11.1 above, in cases where more than 25 % of the vessel's personnel have been changed with personnel that have not previously participated in any security drill on that vessel within the last three (3) months, a vessel security drill shall be conducted within one week of such a change.

11.3 The Company shall conduct an annual company security exercise, with no more than 18 months between the exercises, with one or more vessels 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.

12. Barbados Vessels 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 vessel 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 vessel has a designated SSO who is not the Master. The completed Declaration of Security shall be retained as per Sec. 6.8 above.

12.2 The vessel shall implement additional security measures to the extent that the CSO and/or SSO and/or Master deem necessary, and at the least:

.1 Implement measures per the SSP equivalent to security level 2 or higher;

.2 ensure all access points to the vessel are guarded;

.3 attempt to execute a Declaration of Security; and

.4 Log all implemented security measures for potential review by authorities at future port calls.

13. Verification and Certification

13.1 Interim, initial, intermediate and renewal verifications that shall be conducted as required by the ISPS Code, Part A, Sec. 19.

13.2 The Barbados RSO that issues the International Ship Security Certificate (ISSC), with a validity of five (5) years shall be consulted if changes are made to security systems, equipment, or the approved SSP.

13.3 A vessel detained on maritime security grounds must undergo an additional verification before being allowed to sail.

13.4 An interim ISSC can be issued after an Interim Verification:

.1 to new vessels on delivery;

.2 when a Company takes responsibility for the operation of a vessel which is new to the Company; or

.3 when a vessel changes flag.

13.5 Interim ISSCs are issued for a period not exceeding 6 months. The BMSR 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.

13.6 On satisfactory completion of the initial verification the Barbados RSO can issue a full-term ISSC.

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

13.8 The Barbados RSO or company shall send copies of any type of ISSC to the BMSR.

13.9 The intermediate verification shall be taking place between the second and third anniversary date of the issue of the ISSC and if not done within the window, the ISSC becomes invalid as per ISPS Code, Part A, Sec. 19.3.8. 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. This is to be done in consultation with the BMSR as per Sec 13.15 below.

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

13.11 When the renewal verification is completed within three months before the expiry date of the existing ISSC, the new ISSC 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 ISSC.

13.12 When the renewal verification is completed more than three months before the expiry date of the existing ISSC, the new ISSC 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. This is to be done in consultation with the BMSR as per Sec 13.15 below.

13.13 If a renewal verification has been completed and a new ISSC cannot be issued or placed on board the vessel before the expiry date of the existing ISSC, the RSO may endorse the existing ISSC, and such an ISSC will be accepted as valid for a further period which shall not exceed five months from the expiry date. This is to be done in consultation with the BMSR as per Sec 13.15 below.

13.14 If a vessel at the time when an ISSC expires is not in a port in which it is to be verified, the BMSR may extend the period of validity of the ISSC upon receiving an application through RSO, but this extension will be granted only for the purpose of allowing the vessel to complete its voyage to the port in which it is to be verified, and only in cases where it appears proper and reasonable to do so. No ISSC will be extended for a period longer than three months, and the vessel 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 ISSC. 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 ISSC before the extension was granted.

13.15 When the intermediate or renewal verifications cannot be done within the due time frame and in the cases of the Sec. 13.9, 13.12 and 13.13 above the RSO shall contact the BMSR for issuance of a permit as per Sec. 5 of Bulletin 008.

Revision No	Description Of Revision
1.0	First Issue – Revoke Bulletin 334 : Ship Security Alert Systems (SSAS) Rev.1.0