
Circular 2011/002

Amendments to the Ship Security Plan (SSP)

Date: 11-09-2018

To whom it may concern,

This circular is applicable to all ships on which Chapter XI-2 of SOLAS (ISPS Code), as amended, and/or Regulation 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, as amended, is applicable.

This circular refers to 'BMI circular 2004/002 ISPS - Flagstate interpretations and procedures' in regard of the Recognized Security Organizations and the provisions set down in the working agreement between the Belgian Maritime Inspectorate (BMI) and the recognized classification societies related to the application of the ISPS Code.

Regulation A/9.5 of the ISPS Code states:

*'The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall **not** be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this Part of the Code.'*

Any amendment, as mentioned in article 9.5 of Part A of the ISPS Code and article 1.12 of part B of the ISPS Code, which has an effect on the security of the vessel, needs to be notified by the Company Security Officer (CSO) to the Recognized Security Organization (RSO) involved. In doing so the CSO has to indicate also the implications of the proposed amendment(s).

The RSO decides if the change(s) may be implemented, and if so, under which circumstances.

Any change should provide at least equal or higher security level.

Although the RSO may decide if a change may be implemented or a re-approval of the SSP is required prior the implementation, taking into account the requirements of this circular, BMI reserves the right to take this decision by itself. In such case the RSO will be informed accordingly.

In accordance with the working agreement between BMI and the recognized classification societies, acting as RSO's, the RSO's are authorized to carry out the re-approval of the SSP on behalf of Belgium.

Upon completion of the re-approval of the SSP, the RSO should re-issue the approval letter which should be countersigned by BMI and included in the SSP.

The attached table in annex contains the amendments which in any case require the re-approval of the SSP by the RSO and the method on which the evaluation needs to be carried out.

Minor editorial changes to the SSP, including changes to the document control system, do not require a re-approval of the SSP. This may include the following:

- Changes to telephone numbers in connection with handling of security related events on board Belgian flagged vessels;
- Changes to addresses in connection with handling of security related events on board Belgian flagged vessels;
- Changes to names of the Company Security Officer and/or his deputy;
- Changes to and updating of existing ISM documents already approved in the annex as a part of the SSP;
- Changes to the format of check lists.

It is of utmost importance that security-related information is updated as soon as any changes occurs.

It is to be noted that an SSP cannot be approved before the date of the registration of the ship.

In case of changes, the Belgian Maritime Inspectorate should be informed as soon as possible via the following email address: Ship.Belflag@mobiliteit.fgov.be

Certain documents from the ISM system can be accepted during the approval of the SSP as an annex to the SSP since there is no need for duplication of documents.

Any questions regarding ISPS may be directed to: Belgian Maritime Inspectorate
Ship.Belflag@mobiliteit.fgov.be
Posthoflei 3-5
2600 Berchem
Belgium

ir.Bart Heylbroeck
Naval Architect - Director
Belgian Maritime Inspectorate

ANNEX

Nr	Relevant part of the SSP	Approval
1	Procedure regarding the confirmation of a change in security level	1
2	Security measures taken at security level 2 and 3	2*
3	Reporting of security incidents to CSO, Flagstate, Port- and Coastal state authorities.	1
4	Frequency of testing and calibration of security equipment	1
5	Drills and exercises, and security briefings	1
6	Verification (audits) of the security measures and SSP, including the frequency of the verifications	1
7	Review of the SSP	1
8	Records (which, how and where are they kept)	1
9	Procedures to prevent unauthorized access to the SSA, SSP and records	1
10	Identification of restricted areas	2
11	Protocols and other procedures to access the restricted areas	1
12	Procedure for the use of security equipment	1
13	Illumination of deck and access points	2*
14	Procedures for watch keeping an access control at each security level	1
15	Arrangements with regard to security assistance from shore (such as patrol, guards...)	1
16	Maintenance procedures for security equipment	1
17	Ship Security Alert System (SSAS): all related issues such as type, location, activation points, receivers,...etc	2
18	For ships with a restricted sailing area a new SSA must be performed in case the ship is getting repositioned to a location which is not covered within the SSA.	1

Clarification on method of approval

1. Evaluation based on documentation
2. Evaluation based on documentation and verification on board
- 2*. Evaluation based on documentation, and as far as practical, verification on board