DMA RSO Circular no. 007

ISPS and SSAS

Rule reference

- SOLAS, chapter XI-2 and Regulation (EC) no. 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security.

Explanatory note

This circular contains guidance on the Ship Security Alert System (SSAS) and on changes to the Ship Security Plan (SSP) in accordance with the abovementioned regulations.

This circular repeals the DMA guidance no. 007 on ship security alert systems revision 01 of 11 September 2020.

Guidance on SSAS

Setting up of security alerts in Danish ships

The Danish Maritime Authority has, in cooperation with the Royal Danish Navy Command, determined the course of action for security alerts and hereby provides the guidelines.

All security alerts from Danish ships shall be:

- Submitted to Danish Maritime Assistance Service (MAS) without any delay,
- Addressed to MAS' land-mobile Inmarsat C system and their email address, and
- Submitted to the Company Security Officer (CSO).

The coding of the address field shall have the following order of priority on Inmarsat-C terminals:

1. 492380442 (Land Inmarsat-C)
2. Contact of the Company Security Officer
3. E-mail to MAS (mas@sok.dk)

The coding of the address field shall have the following order of priority on Iridium terminals:

1. 492380442@c12.stratosmobile.net
2. Contact of the Company Security Officer
3. E-mail to MAS (mas@sok.dk)

Ship identification

The ship shall be identified clearly and unambiguously in the security alert. The message shall contain at least the following information:

- **IMO no.**
- **MMSI no.**
- **Ship's name**
- **Call sign**
- **Date/time zone (updated automatically and continuously)**
- **Position, course, and speed, if relevant (updated automatically and continuously)**

Testing of security alerts on Danish ships

To ensure the functionality of the system, a live alert shall be submitted to MAS after the installation is completed – or if any major changes are made to the system's set-up. Furthermore, live alert shall be submitted in connection with the periodic survey of the radio installation or during an ISPS audit.

Carrying out the live alert test

The master, an officer, or a surveyor from a recognized security organization should carry out the live alert test. Before the test, the following steps must be carried out:

1. Inform MAS by e-mail (mas@sok.dk) from the ship no earlier than 48 hours in advance.
2. Contact MAS by phone (+45 72 85 03 70) immediately prior to testing, in order to get MAS' approval to carry out the test.

After activating the SSAS, MAS will contact the ship to confirm reception of the alert.

During the periodic survey on Inmarsat-C terminals, it should also be ensured that ships carrying Inmarsat-C terminals has encoded ENID number 28941 in the primary Inmarsat-C terminal. Please see Guidance no. 9253 of 28 June 2011 on important messages (OXXO) via Inmarsat-C as amended.

In case of unintentional activation of the SSAS, MAS must be contacted immediately.
(tel. +45 72 85 03 70)

In addition to the mentioned live alert test, the SSAS should be tested internal regularly. Procedures, instructions and guidance on the use of the SSAS, including the testing, activation, deactivation and resetting and to limit false alerts, should be kept in the SSP as per Regulation (EC) no. 725/2004, part A, paragraph 9.4.18.

Please observe that internal test alerts shall not be sent to MAS.

Documentation for the testing of the SSAS

Both the annual live alert test and the internal test shall be documented on board in the ISPS security records.

Company Security Officer List

All Danish shipping companies shall inform MAS (mas@sok.dk) about the name and contact information of all appointed CSOs. It is important that MAS is in possession of the accurate contact information at all times. The shipping company is responsible for updating MAS with the appropriate contact information.

Reception of Ship Security Alarm through service providers

Danish shipping companies can send ship security alerts through a communication service provider (CSP) directly to MAS, as described above.

If a CSP is used, it must be ensured that the service provider is operational at all times, 24/7/365, to ensure reliable transmission of the ship security alert to MAS.

The shipping company using a CSP must have a service agreement with the applicable CSP.

During initial, intermediate and renewal audit, the recognized security organizations are obliged to verify that a service agreement between the relevant Danish shipping company and the applicable CSP are in place.

The requirements for live alert test of the SSAS are the same as described above.

Security related information from Danish Authorities

The recognized security organizations are obliged to verify, that Danish ships carrying Inmarsat-C terminals comply with Guidance no. 9253 of 28 June 2011 on important messages (OXXO) via Inmarsat-C as amended.

MAS will communicate security related information to Danish ships through OXXO messages as well as the CSO list.

Security Level in Denmark

The Danish Ministry of Defence is the responsible authority for determining the MARSEC security level in Danish waters and on board Danish ships. MAS will communicate any change in the security levels on board Danish Ships and in Danish waters.

Changes to the Ship Security Plan

Danish requirement

The Danish Maritime Authority requires all changes to the Ship Security Plan (SSP) to be forwarded for re-approval, except for the following:

- Minor editorial changes to the SSP, including changes to the document control system.
- Changes to telephone numbers.
- Changes to names and responsible persons.
- Changes to physical addresses.
- Changes to e-mail addresses and websites.
- Changes to the format of checklists (records).
- Changes to and updates of existing ISM documents already approved in the annex as a part of the ISPS manual[1]

Generically preapproved SSASs must be specified on ship level.

The company may have a number of SSASs preapproved for use in its fleet in a generic version of the SSP.

When approving an individual SSP, multiple SSASs are acceptable, but only the sections of the SSP relevant to the alert system currently installed on board must be available on board. There must be no doubt about what type, make and configuration of SSAS is used on board.

ISPS Security Records

In accordance with regulation (EC) no. 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, part a, paragraph 10.1.2, the ISPS Security Records shall be kept on board for at least the minimum period specified by the Administration.

[1]During approval of an updated SSP, certain documents from the ISM system can be accepted as an annex to the SSP, as there is no need for duplicate documents.

The minimum period set by the administration is 3 years for ships flying the flag of an EU Member State.

Issuance of an interim ISSC

Issuance of an interim ISSC must be done in accordance with regulation (EC) no. 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, part a, paragraph 19.4.