REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-18

Rev. Jan/2023

TO: **ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS, AND RECOGNIZED ORGANIZATIONS**

SUBJECT: **Ship Security Alert System (SSAS)**

References:

(a) **SOLAS,** *International Convention for the Safety of Life at Sea, Consolidated Edition 2020*

(b) **ISPS Code**, *International Ship and Port Facility Security (ISPS) Code*

(c) **ISM Code**, *International Safety Management (ISM) Code*, 2018 edition

(d) **IMO Resolution** MSC.147(77), *Adoption of the revised performance standards for a Ship Security Alert System*, adopted 29 May 2003

(e) **IMO Circular** MSC.1/Circ.1072, *Guidance on provision of Ship Security Alert Systems*, issued 26 June 2003

(f) **IMO Circular** MSC.1/Circ.1155, *Guidance on the message priority and the testing of Ship Security Alert Systems*, issued 23 May 2005

(g) **IMO Circular** MSC.1/Circ.1190, *Guidance on the provision of information for identifying ships when transmitting Ship Security Alerts*, issued 30 May 2006

(h) **RMI Marine Notice** 2-011-16, *International Ship and Port Facility Security (ISPS) Code*

(i) **RMI Marine Guideline** 2-11-15, *Organizations Acting on Behalf of the Republic of the Marshall Islands Maritime Administrator*

PURPOSE

This Notice provides the requirements for the Ship Security Alert System (SSAS), in accordance with SOLAS chapter XI-2, regulation 6 as installed on Republic of the Marshall Islands (RMI)-flagged vessels. It sets forth the policy that, effective 1 April 2017, the RMI Administrator (the "Administrator") will no longer receive SSAS alerts directly from any RMI-flagged vessel.

This Notice supersedes Rev. Oct/2021. Ship Security has undergone a name change to Maritime Security and its new email address is: marsec@register-iri.com.

APPLICABILITY

In accordance with SOLAS chapter XI-2, regulation 6, all ships on international voyages in the general categories listed below, must have an SSAS installed on board. This includes:

- passenger ships, including high-speed passenger craft;
- cargo ships, including high-speed craft, of 500 gross tons and upwards; and
- mechanically-propelled mobile offshore drilling units as defined in SOLAS chapter IX, regulation 1, not on location.

DEFINITIONS

Company means the owner of the ship or any other organization or person, such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who, on assuming such responsibility, has agreed to take over all the duties and responsibilities imposed by the International Safety Management (ISM) Code.

Competent Authority means the entity responsible for receiving SSAS transmissions. The Administrator has designated the Competent Authority to be either the Company Security Officer (CSO) or Alternate Company Security Officer (ACSO) or a Company-designated qualified third party.

False Alert means an unplanned alert transmitted by accident.

Real Alert means an unplanned alert transmitted during an actual security incident, threat, or perceived threat.

Test Alert means a planned alert transmitted to ensure that the SSAS equipment is functional and properly programmed (e.g., initial installation, ISPS Code verification audits, security exercises and drills, or prior to entering an area of high risk).

REQUIREMENTS

1.0 Ship Security Alert System

1.1 In accordance with SOLAS chapter XI-2, regulation 6, activation of the Ship Security Alert System (SSAS) must initiate and transmit a ship-to-shore security alert to a Competent Authority indicating that the security of the ship is under threat or has been compromised.

1.2 It is the Administrator's policy that the Competent Authority is responsible for receiving SSAS transmissions and determining whether the alert is real, test or false.

1.3 The Competent Authority must be identified in the Ship Security Plan (SSP).

1.4 The SSAS is a requirement of SOLAS chapter XI-2 and is not considered to be radio equipment. Therefore, it is not covered by the Safety Radio Survey and the Safety Radio Certificate is not affected. However, any defect or malfunction in the SSAS is considered a failure of compliance with the ISPS Code.

2.0 Designation of a Competent Authority

2.1 The Company must designate either an internal appointee (the Company Security Officer (CSO) or Alternate Company Security Officer (ACSO)) or an external, qualified third party to serve as the Competent Authority.

2.2 To be considered qualified, a Competent Authority must:

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

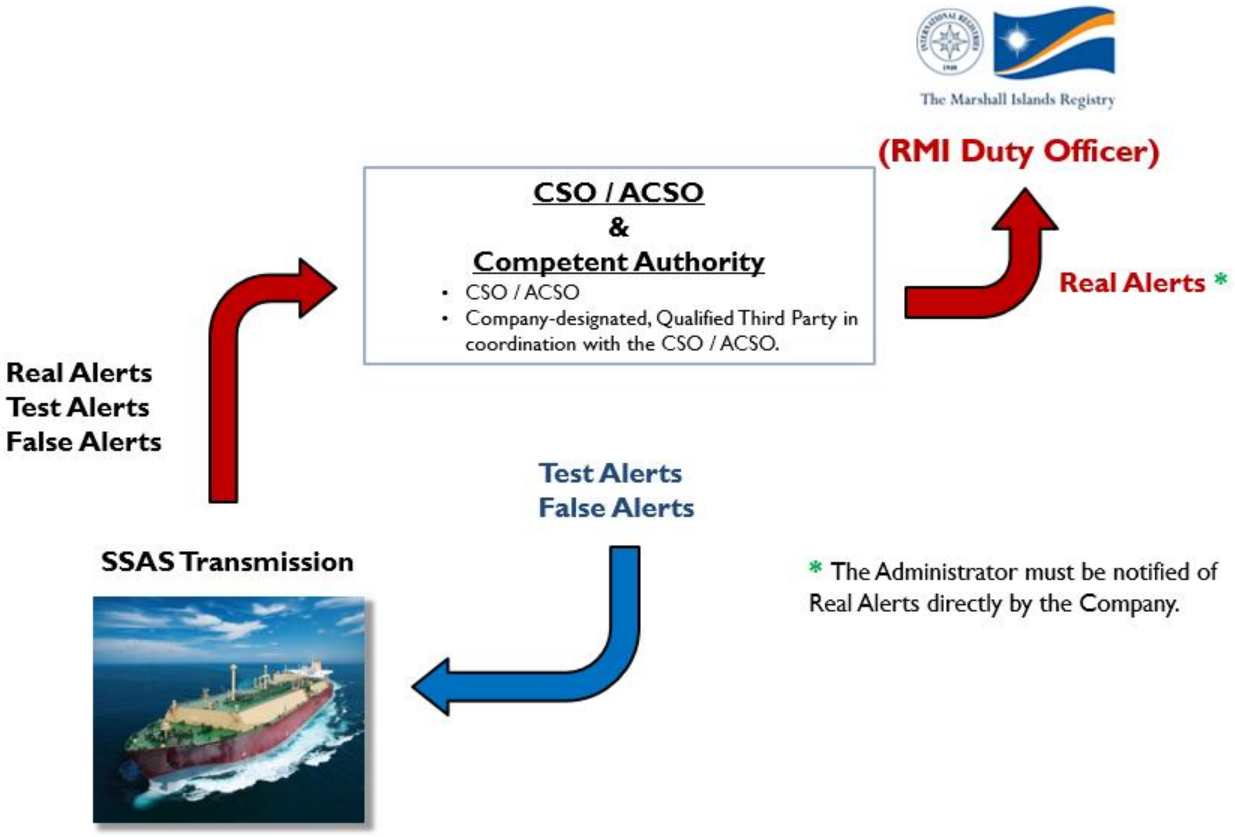
.2 be able to accurately identify and react to real, test, or false alerts;

.3 understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code and the Administrator's SSAS requirements contained herein;

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

.5 participate in exercises involving tests of the SSAS.

2.3 The Competent Authority must directly receive and respond to all SSAS alerts, ensure proper functioning of the SSAS equipment, and verify the completeness and accuracy of the transmitted data without the need for receipt or acknowledgement by the Administrator. The diagram below summarizes how the Competent Authority must handle and respond to SSAS transmissions.



2.4 Administrator involvement must be reserved only for SSAS transmissions that are determined to be real alerts. These must be immediately forwarded by the Company to the Administrator to fulfill its duties required by SOLAS chapter XI-2, regulation 6.

.1 The Company must immediately notify the Administrator of a **real alert** by contacting:

.a the RMI Duty Officer (Tel: +1 571 441 1885); or

.b via email: dutyofficer@register-iri.com.

.2 Third party Competent Authorities must not contact the Administrator directly. All direct communication with the Administrator must be from the Company.

.3 Non-emergency follow-up communication regarding a security incident must be sent to the Administrator at marsec@register-iri.com.

2.5 CSOs are required to verify that each SSAS installed on board an RMI-flagged vessel has been correctly programmed to transmit all SSAS alerts directly to the Competent Authority as defined in §1.1.

3.0 SSAS Testing by the Company

3.1 Following the initial installation of the SSAS, the Company must:

.1 ensure that the system is tested and maintained to satisfy operational requirements per the approved SSP; and

.2 keep on board the records specified in ISPS Code Part A, §10.1.10.

3.2 The system must be tested annually to verify proper operation. Testing must include the entire alert system, from activation to the alert's receipt by the Competent Authority. On completing the test, the SSAS must be reset.

3.3 The unit must be capable of being testing in the presence of a port State control inspector on request, but only from the required navigation bridge location and with appropriate prior notification of the Competent Authority.

3.4 The procedure for SSAS testing must be outlined in the SSP or in a separate document to avoid compromising its confidentiality. This separate document must be available only to the Master, Ship Security Officer (SSO), or Alternate SSO.

3.5 If possible, test alerts must be marked "TEST."

3.6 SSAS testing must be properly logged in the vessel's Official Log.

3.7 The SSAS test must be carried out when changing management or the flag.

4.0 SSAS Transmission

4.1 Security alert transmissions must not be included with any other routine reporting that the ship may conduct.

.1 The alert transmission must be generated automatically with no input from the vessel or Company other than the activation of the system and must be transmitted to the CSO/ACSO and third party (if applicable).

.2 Cellular or mobile telephones may not be sufficiently automated to satisfy this requirement. Compliance is required with MSC.1/Circ.1190 and RMI requirements.

4.2 The SSAS transmission must be able to reach the Competent Authority from any point along the vessel's intended route. The SSAS alert must not be transmitted as a general distress call and must be sent directly to the Competent Authority. The CSO/ACSO must be a recipient of all SSAS alerts, even if the CSO/ACSO is not the designated Competent Authority.

4.3 All SSAS messages received by the Competent Authority, and determined to be real, must be immediately forwarded by the Company to the Administrator. These messages must include this ship 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

5.0 SSAS Activation

5.1 Activating an alert must require only a single action, excluding the opening of protective covers. There must be at least two activation points. One must be on the navigation bridge and at least one other in an area where it would normally be immediately accessible.

.1 The activation points must not be able to deactivate the alert once initiated and must be protected against inadvertent operation.

.2 The activation point must not be protected by seals, lids, or covers that must be broken to activate the alert since a broken seal would indicate the alert has been tripped.

.3 Spring-loaded covers or similar devices that provide no indication of the status of the alert are acceptable.

5.2 Once activated, the SSAS must continue to transmit the security alert not less than once every 30 minutes until its status is confirmed by the Competent Authority and the CSO/ACSO gives authorization to reset or deactivate the SSAS.

.1 There must be a confidential procedure in place to properly verify the status of the alert and any resetting or deactivating of the SSAS.

.2 The vessel must initiate the system deactivation unless this can be remotely done by the CSO/ACSO.

6.0 SSAS Performance Standards and Functional Requirements

6.1 Performance standards for the SSAS are detailed in IMO Resolution MSC.147(77). Circulars MSC/Circ.1072 and MSC/Circ.1155 provide further guidance on the SSAS design and functional requirements.

6.2 Due to the mode of installation and operation, there are effectively two types of systems, commonly known as the SSAS and the Self-Contained SSAS (SSAS-SC). Companies must be aware of which type is fitted to their vessels, so the appropriate software is used. This will help to ensure that the Competent Authority receives all required information listed in §4.3 above.

6.3 The SSAS should be powered from the vessel's main and alternative source of power. Alternative source of power is either emergency power supply, a storage battery charged with emergency power source, or independent battery.

7.0 Ship Security Plan (SSP)

7.1 The SSP is a requirement of the ISPS Code, and its preparation is covered in RMI Marine Notice 2-011-16.

7.2 SOLAS vessels are required to have SSAS procedures documented in their SSP. The vessel's SSAS equipment and procedures will be reviewed in conjunction with the vessel's SSP.

7.3 The ISPS Code requires that the activation point locations be identified in the SSP. To avoid compromising the objective of the SSAS, this location information may be kept elsewhere on board in a document known only to the Master, SSO, and other senior shipboard personnel as may be decided by the Company.

7.4 The SSP may need to be amended to reflect the handling of SSAS transmissions per §2.2 and §2.3, including the deletion of any Administrator email address. The testing of any newly programmed SSAS settings must be done to the satisfaction of the Competent Authority. Any respective SSP amendment regarding reprogramming of the SSAS must be reviewed and verified during a scheduled ISPS Code verification audit.

8.0 Shipboard Verification

8.1 During the ISPS shipboard verification following the initial installation of the SSAS, the maritime security auditor must review and approve the related provisions in the SSP, witness a complete security alert test and verify the implementation of the operational requirements of the SSAS in accordance with the requirements of ISPS Code Part A, §§9.4.17 - 9.4.18.

8.2 During each subsequent ISPS verification, the maritime security auditor must examine the activity records of the SSAS or SSAS-SC as specified in ISPS Code Part A, §10.1.10. The auditor must also witness a complete SSAS test alert during each ISPS verification.

8.3 A complete SSAS test alert must include transmission of a test message to the CSO, the Competent Authority, or both.

8.4 A list of Recognized Security Organizations authorized to act on behalf of the Administrator can be found in MG 2-11-15.