REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-18

Rev. Mar/2017

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 2014*, as amended

(b) **ISPS Code**, *International Ship and Port Facility Security (ISPS) Code*, 2003 edition, as amended

(c) **ISM Code**, *International Safety Management (ISM) Code*, 2014 edition, as amended

(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/Circ.1072,** *Guidance on Provision of Ship Security Alert Systems*, dated 26 June 2003

(f) **IMO Circular MSC/Circ.1155,** *Guidance on the Message Priority and the Testing of Ship Security Alert Systems*, dated 23 May 2005

(g) **IMO Circular MSC/Circ.1190,** *Guidance on the Provision of Information for Identifying Ships When Transmitting Ship Security Alerts*, dated 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 the International Convention for the Safety of Life at Sea (SOLAS), Regulation XI-2/6, as installed on Republic of the Marshall Islands (RMI) flagged vessels. It sets forth the policy that, effective 01 April 2017, the RMI Administrator (the "Administrator") will no longer receive SSAS alerts directly from any RMI flagged vessel.

This Notice supersedes Rev. 7/15. Concurrently, Marine Guideline 2-11-11 has been revoked.

Inquiries concerning the subject of this Notice should be directed to the Republic of the Marshall Islands Maritime Administrator, c/o Marshall Islands Maritime and Corporate Administrators, Inc., 11495 Commerce Park Drive, Reston, VA 20191-1506 USA. The most current version of all Republic of the Marshall Islands Marine Notices may be found at www.register-iri.com.

APPLICABILITY

In accordance with SOLAS Regulation XI-2/6, all ships on international voyages, in the general categories listed below, shall have an SSAS installed on board:

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

.2 Cargo ships, including high-speed craft, of 500 gross tons and upwards; and

.3 Mechanically propelled mobile offshore drilling units as defined in SOLAS IX/1, not on location.

REQUIREMENTS

1.0 SSAS

1.1 In accordance with SOLAS Regulation XI-2/6, activation of the SSAS shall initiate and transmit a ship-to-shore security alert to a Competent Authority[1] 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 shall be responsible for receiving SSAS transmissions and determining whether the alert is real[2], test[3] or false[4].

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

1.4 The SSAS is a requirement of SOLAS 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 International Ship and Port Facility Security (ISPS) Code and potentially the International Safety Management (ISM) Code.

---

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

2 *Real Alert* shall mean an unplanned alert transmitted during an actual security incident, threat, or perceived threat.

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

4 *False Alert* shall mean an unplanned alert transmitted by accident.

2.0 Designation of a Competent Authority

2.1 The Company[5] shall 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 upon SSAS alerts;

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

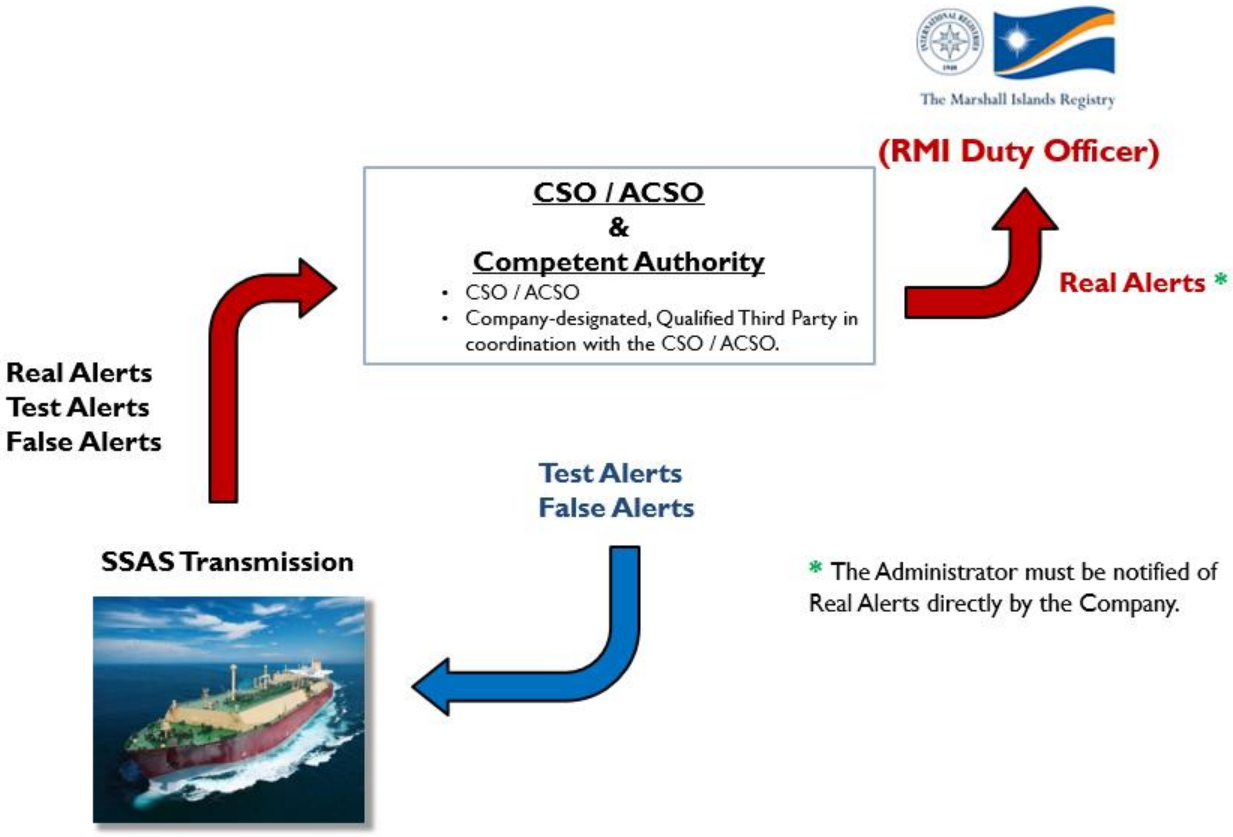
.3 understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code and the Administrator's SSAS requirements contained herein;

.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 drills or exercises involving tests of the SSAS.

2.2 The Competent Authority shall directly receive and respond to all SSAS alerts, ensuring proper functioning of the SSAS equipment and verifying 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 shall handle and respond to SSAS transmissions.

[5] *Company* shall mean 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.


The Marshall Islands Registry
(RMI Duty Officer)
CSO / ACSO
&
Competent Authority
• CSO / ACSO
• Company-designated, Qualified Third Party in coordination with the CSO / ACSO.
Real Alerts *
Real Alerts
Test Alerts
False Alerts
Test Alerts
False Alerts
SSAS Transmission
* The Administrator must be notified of Real Alerts directly by the Company.

2.3 Administrator involvement shall be reserved only for SSAS transmissions that are determined to be real alerts. Real alerts must be immediately forwarded by the Company to the Administrator so it may fulfill its duties required by SOLAS XI-2/6.

.1 The Company shall immediately notify the Administrator of a **real alert** by contacting the **RMI Duty Officer**.

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

.3 Non-emergency, follow-up communication regarding a security incident shall be sent to the Administrator's Ship Security department at shipsecurity@register-iri.com.

2.4 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 shall:

.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 A/10.1.10.

3.2 The system shall be capable of being tested to verify proper operation. Testing must include the entire alert system, from activation to receipt of the alert by the Competent Authority. Upon completion, the test must also include resetting of the SSAS.

3.3 The unit must also be capable of being tested in the presence of a port State control inspector upon 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 document separate from the SSP to avoid compromising its confidentiality. This separate document shall be available only to the Master, SSO, or Alternate SSO.

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

3.6 Testing of the SSAS shall be properly logged in the vessel's Official Log.

4.0 SSAS Transmission

4.1 The transmission of a security alert is not to be included with any other routine reporting

that the ship may conduct. 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). Cellular telephones may not be sufficiently automated to satisfy this requirement. Compliance with MSC/Circ.1190 and RMI requirements is compulsory.

4.2 The SSAS transmission must be capable of reaching the Competent Authority from any point along the vessel's intended route. An SSAS alert is not to be transmitted as a general distress call, and is to 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. Such messages must include the following ship information:

.1 Vessel Name;

.2 IMO Ship Identification 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 The activation of an alert shall only require a single action, excluding the opening of protective covers. There must be at least two (2) activation points. One (1) must be located on the navigation bridge and at least one (1) other in an area where it would normally be immediately accessible. The activation points shall not be capable of deactivating the alert once initiated and must be protected against inadvertent operation. 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 that the alert has been tripped. Spring loaded covers or similar devices that provide no indication of the status of the alert are acceptable.

5.2 Once activated, the SSAS shall continue to transmit the security alert at a frequency of not less than once per 30 minutes until the status of the alert is confirmed by the

Competent Authority and authorization is given by the CSO/ACSO for the alert to be reset or deactivated. There shall be a confidential procedure in place to properly verify the status of the alert and any resetting or deactivation of the SSAS. The vessel shall initiate the deactivation of the system, unless it can be remotely deactivated 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 design and functional requirements of the SSAS.

6.2 Due to the mode of installation and operation, there are effectively two (2) types of systems, commonly known as the SSAS and the Self-Contained SSAS (SSAS-SC). Companies should be aware of the difference and which type they have fitted to their ships so that the appropriate software and interfaces are provided to ensure that the Competent Authority receives all required information listed in §4.3 above.

6.3 The SSAS should be powered from 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 therefore be reviewed in conjunction with the vessel's SSP. Although the ISPS Code requires that the location of the activation points be identified in the SSP, it also provides that, in order to avoid the possibility of compromising the objective of the SSAS, this information may be kept elsewhere on board in a document known only to the Master, Ship Security Officer (SSO), and other senior shipboard personnel as may be decided by the Company.

7.3 The SSP may need to be amended to reflect the handling of SSAS transmissions as per §2.2 and §2.3 above, including the deletion of any Administrator email address. The testing of any newly programmed SSAS settings shall be conducted to the satisfaction of the Competent Authority and any respective SSP amendment in regards to reprogramming of SSAS shall be reviewed and verified during the next scheduled ISPS Code verification audit after 01 April 2017.

8.0 Shipboard Verification

8.1 At the ISPS ship board verification following the initial installation of the SSAS, the auditor shall 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 A/9.4.17 to A/9.4.18.

8.2 At each subsequent ISPS verification the auditor shall examine the records of activities on the SSAS or SSAS-SC as specified in ISPS Code A/10.1.10. The auditor shall also witness a complete SSAS test alert during each ISPS verification.

8.3 A "complete" SSAS test alert shall include transmission of a test message to the CSO and/or Competent Authority.

8.4 A list of RSOs authorized to act on behalf of the Administrator can be found in RMI Marine Guideline 2-11-15.