Republic of the Marshall Islands

MARITIME ADMINISTRATOR

11495 COMMERCE PARK DRIVE, RESTON, VIRGINIA 20191-1506
TELEPHONE: +1-703-620-4880 FAX: +1-703-476-8522
EMAIL: shipsecurity@register-iri.com WEBSITE: www.register-iri.com

SHIP SECURITY ADVISORY No. #01-17

To: **Owners/Operators, Masters, Company Security Officers, Recognized Security Organizations**

Subject: **ADVANCE NOTICE OF POLICY CHANGE - HANDLING OF SHIP SECURITY ALERT SYSTEM TRANSMISSIONS**

Date: **24 January 2017**

This Ship Security Advisory clarifies and supersedes SSA #11-16, which is now revoked.

In accordance with International Convention for the Safety of Life at Sea (SOLAS) Regulation XI-2/6, activation of the Ship Security Alert System (SSAS) shall initiate and transmit a ship-to-shore security alert to the Company-designated Competent Authority, indicating that the security of the ship is under threat or has been compromised. The Company-designated Competent Authority is also responsible for receiving SSAS test messages and investigating whether the alert is real[1], test[2], or false[3]. The Company-designated Competent Authority is defined as the recipient of the SSAS transmissions.

This Advisory serves as advance notice that, effective **01 April 2017,** the Republic of the Marshall Islands (RMI) Maritime Administrator (the "Administrator") will no longer receive SSAS alerts directly from any vessel. The Administrator's new policy will instead provide for the Company[4] **or** a Company-designated qualified third party, to serve as the Competent Authority to receive and verify SSAS transmissions.

This policy change will allow the Company or the Company-designated, qualified third party 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 Administrator.

This reserves Administrator involvement to only those SSAS transmissions that are real, which are to be immediately forwarded by the Company to the RMI Duty Officer. Third party Competent Authorities must not contact the Administrator directly.

See Flowchart in Appendix I

---

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

2 *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) audits, security exercises and drills, or prior to entering a high risk area).

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

4 *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.

This SSA expires one (1) year after its issuance, unless otherwise noted, extended, superseded, or revoked.

REQUIRED CHANGES

1.0 Designation of a Competent Authority

Companies will be required to designate either an internal appointee (preferably the Company Security Officer (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.

.1 To be considered qualified, a Competent Authority must:

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

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

c. Understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code and the Administrator's SSAS requirements contained in RMI Marine Notice 2-011-18;

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

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

2.0 Reprogramming of the SSAS Unit

Companies must ensure that the SSAS unit is reprogrammed so that alerts are only transmitted to the Company-designated Competent Authority. This means that the Administrator's email address ("Y6Z…@register-iri.com") must be removed from the unit's program settings and replaced with that of the Company-designated Competent Authority (internal appointee and/or external third party service).

.1 Other than the deletion of the Administrator's contact information from the programmed alert, all other information in the SSAS alert remains the same as listed below:

a. Vessel Name;

b. IMO Ship Identification Number;

c. Call Sign;

d. Maritime Mobile Service Identity (MMSI) Number;

e. Date and Time;

f. Vessel Position;

g. Course and speed;

h. Name of CSO and 24/7 phone number; and

i. Name of Alternate CSO and 24/7 phone number.

It is recommended that a radio service technician is contacted so that reprogramming of the SSAS unit can be scheduled at a convenient time, possibly along with other routine service, rather than waiting until **01 April 2017**, the date for this policy change.

All SSAS transmissions are to be transmitted only to the CSO and the Company-designated Competent Authority (i.e. CSO/ACSO and qualified third party, if applicable).

3.0 Revisions to the Ship Security Plan and ISPS Code Verification

Companies must ensure that only real alerts are immediately forwarded to the RMI Duty Officer by the CSO so the Administrator may fulfill its duties required by SOLAS Regulation XI-2/6.

Revisions to the Ship's Security Plan (SSP) should be made as may be required. Any changes to the SSP resulting from this change in policy will not require special approval by the Recognized Security Organization (RSO). Initial testing of the new SSAS settings is to be conducted successfully with the Company-designated Competent Authority and documented for the RSO's review during the next scheduled ISPS Code verification audit.

If a vessel has completed reprogramming of the SSAS (as per §2.0) prior to 01 April 2017, live SSAS test alert acknowledgement by the Administrator is not required. If SSAS reprogramming has already taken place, only the Company-designated Competent Authority is required to acknowledge receipt of an SSAS test alert during an ISPS Code verification audit. If SSAS reprogramming has not yet been completed, the Administrator will continue to acknowledge receipt of test alerts only through 31 March 2017.

SCHEDULE TO IMPLEMENT THIS POLICY CHANGE

The Administrator is currently in the process of revising all affected RMI publications to reflect this policy change. **Vessel operators may implement this changed procedure at any time prior to the official implementation date of 01 April 2017**.

Please direct any questions or concerns to shipsecurity@register-iri.com.

SSAS POLICY CHANGE FAQs

1. **The vessel's annual radio survey is scheduled before 01 April 2017. Should the SSAS settings be reprogrammed during the survey?**

   Yes. If the annual radio survey is already scheduled to take place prior to 01 April 2017, this may be a convenient opportunity to reprogram the SSAS unit by removing the Administrator's email address and replacing it with the address of the Company-designated Competent Authority.

2. **The vessel's annual radio survey is scheduled for on or after 01 April 2017. Should we wait until the survey to change the settings?**

   No. The SSAS unit must be reprogrammed prior to 01 April 2017.

3. **What programming changes must be made to the SSAS unit?**

   The Y6Z…@register-iri.com email address must be removed and replaced by the email address of a Company-designated Competent Authority (internal or qualified third party). The CSO must remain a recipient of all SSAS transmissions, regardless of whether he/she is the Company-designated Competent Authority.

4. **Is there a listing of Administrator-approved qualified Competent Authorities?**

   No. There is no listing of approved third-party Competent Authorities. Companies (ISM/ISPS Code Operators) may choose to appoint a qualified third-party Competent Authority. To be considered qualified, a Competent Authority must:

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

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

   c. Understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code and the Administrator's SSAS requirements;

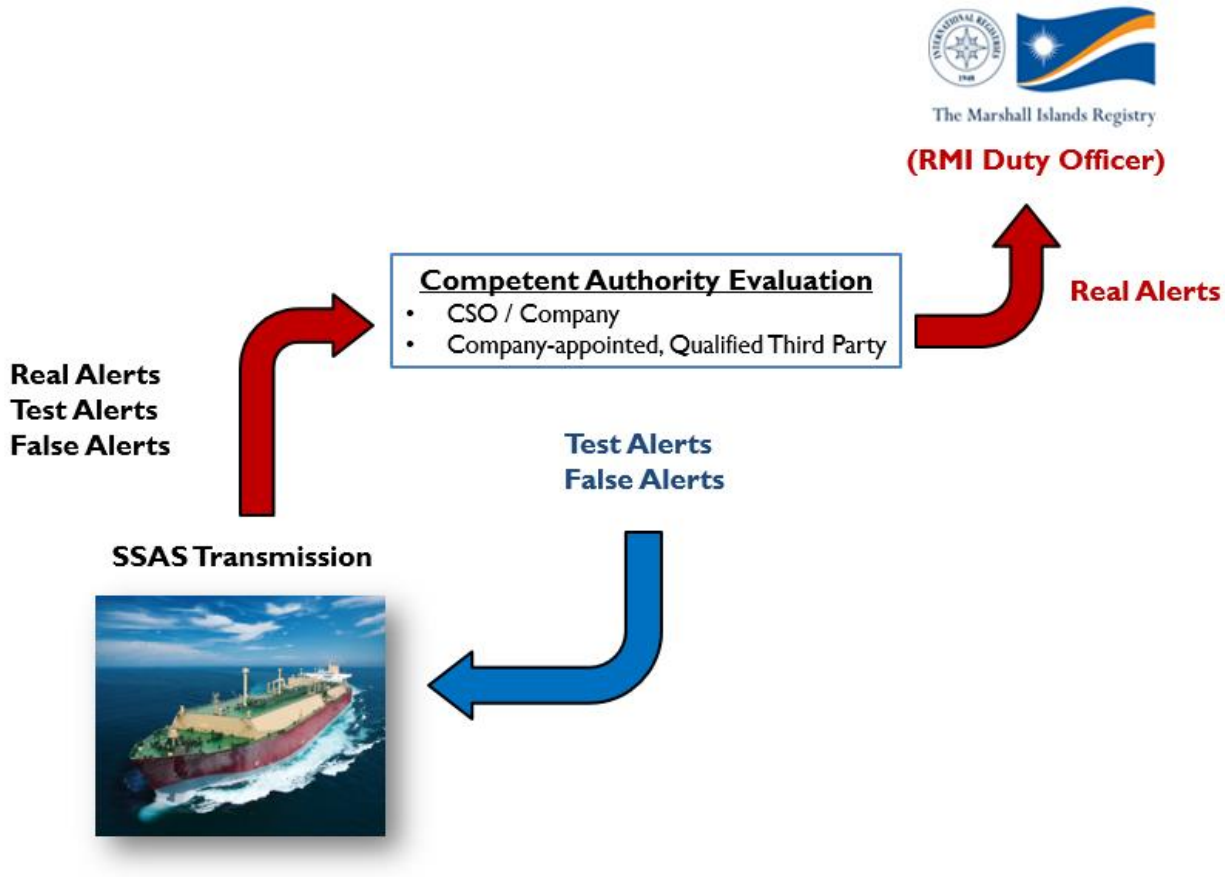
   d. Maintain a current contact list of relevant authorities (Administrator, Maritime Rescue Coordination Centers, Coastal State Authorities, Information Sharing Centers) to be used in the event of an actual alert; and

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

5. **Should a Company-designated third party Competent Authority ever contact the Administrator directly?**

   No. Communication relating to a real SSAS transmission must be sent to the Administrator directly by the Company, preferably the CSO or ACSO. If a third party has been designated as Competent Authority, they must ensure that the Company is alerted. It is then the Company's responsibility to immediately notify the RMI Duty Officer.

APPENDIX I


The Marshall Islands Registry
(RMI Duty Officer)
Competent Authority Evaluation
• CSO / Company
• Company-appointed, Qualified Third Party
Real Alerts
Real Alerts
Test Alerts
False Alerts
Test Alerts
False Alerts
SSAS Transmission