



ST. VINCENT AND THE GRENADINES

MARITIME ADMINISTRATION

CIRCULAR N° ISPS 013 – Rev. 1

GUIDANCE FOR TESTING OF SHIP SECURITY ALERT SYSTEM AND ACTIONS IN CASE OF FALSE ALARM

**TO: COMPANY SECURITY OFFICERS (CSO) / ALTERNATIVE
COMPANY SECURITY OFFICERS, MASTERS, SHIP SECURITY
OFFICERS (SSO), RECOGNIZED SECURITY ORGANIZATIONS**

APPLICABLE TO: SHIPS TO WHICH ISPS APPLIES
ENTRY INTO FORCE: DATE OF THIS CIRCULAR

Monaco, 9th June 2009.

Procedure for testing of SSAS

According to the IMO circular [MSC/Circ.1155](#), companies and ships should ensure that when testing the SSAS with the Flag State, they notify the Flag State 24 hours in advance prior to the test - by sending a notification e-mail to security@svg-marad.com. This is to avoid that the system inadvertently lead to unintended emergency response actions.

In the event of a test, the SSAS alert test message should be configured to have the word "TEST" either in the message or in the subject heading. This is to ensure that the testing of the SSAS does not inadvertently lead to unintended emergency response actions. The alert message should be configured back to the original wordings after the test is completed.

The transmissions of information from the ship's SSAS to St Vincent and the Grenadines Maritime Administration should be limited to information pertaining to actual security alerts and the annual test alert.

Shipowners, Managers and Operators should ensure that internal corresponding e-mails will not be forwarded or listed in copy to security@svg-marad.com. This e-mail should only be receiving pre-test alert notifications and SSAS activation messages.

The procedures for testing the SSAS should be in accordance with MSC/Circ.1155. The frequency of SSAS alert testing involving St Vincent and The Grenadines Maritime Administration should not occur more than once a year and should coincide with the Annual Safety Radio and Safety Equipment Survey.

It is understood that some service providers relating to the shipboard SSAS are providing reports on vessels' location, positions and other data on a regular basis to the CSO and companies as an automatic update. It should be noted that St Vincent and The Grenadines Maritime Administration does not need to be included as a recipient for such information.

SSAS recipient details

Ship Security Alerts, where these are required to be fitted, should be programmed to send a message to the CSO responsible for the vessel, and also to this Administration on security@svg-marad.com only.

Please note that other e-mail addresses which belong to this Administration such as geneva@svg-marad.com or monaco@svg-marad.com should not be used as additional or alternative SSAS recipients. We urge Company Security Officers to check the SSAS settings and delete these addresses accordingly.

Procedure in case of transmitting false SSAS message:

In instances where the SSAS equipment is verified to be faulty and continues to transmit repeated false alerts, **the designated CSO should notify this Administration by e-mail at security@svg-marad.com** and make urgent arrangements with shore maintenance staff to rectify the technical fault as soon as practically possible.

It has been noted that false SSAS messages transmitted out of working hours or during week-ends/holidays were not communicated to this Administration and were rectified on the subsequent working day. These false SSAS messages should be promptly communicated by the CSO to security@svg-marad.com and rectified as soon as possible.

It is also compulsory for the CSO to notify this Administration when the SSAS equipment has been restored to normal operation at the same e-mail address.

In the event that a false alert is inadvertently transmitted, immediate actions should be taken by the CSO to ensure that all parties concerned are informed that the alert is false and that no emergency actions are initiated.

Not reporting immediately false alerts to St Vincent and the Grenadines Maritime Administration, is a non-compliance with SSAS testing procedure and wrong SSAS recipient setting may result in penalties.

The direct telephone relating to SSAS test alerts and SSAS activation is +41 79 447 96 76. Please note that this number is also dedicated to security emergency purposes.



Ref. T2-MSS/2.11.1

MSC/Circ.1155
23 May 2005

**GUIDANCE ON THE MESSAGE PRIORITY AND THE TESTING
OF SHIP SECURITY ALERT SYSTEMS**

1 The Maritime Safety Committee (the Committee), at its seventy-eighth session (12 to 21 May 2004), instructed the Sub-Committee on Radiocommunications and Search and Rescue (COMSAR Sub-Committee) to consider questions relating to the message priority and the testing of ship security alert systems and to develop, if necessary, guidance to this end.

2 The COMSAR Sub-Committee, at its ninth session (7 to 11 February 2005), considered the matter and submitted its recommendations on the issue to the Committee.

3 The Committee, at its eightieth session (11 to 20 May 2005), considered the recommendation of the COMSAR Sub-Committee and approved the Guidance on the message priority and the testing of ship security alert systems (the Guidance), as set out at annex.

4 SOLAS Contracting Governments are invited to bring the Guidance to the attention of all parties concerned with matters relating with ship security alerts and systems.

5 SOLAS Contracting Governments, international organizations and non-governmental organizations with consultative status which encounter difficulties with the implementation of the Guidance should bring, at the earliest opportunity, the matter to the attention of the Committee for consideration of the issues involved and decision on the actions to be taken.

ANNEX**GUIDANCE ON THE MESSAGE PRIORITY AND THE TESTING
OF SHIP SECURITY ALERT SYSTEMS****I Message priority**

1 The Committee, being aware of the message priority requirements applicable to satellite communications, and given the diversity of ship security alert systems, agreed that there was no need to develop a message priority requirement for ship security alerts.

2 Ship security alert system communication service providers should deliver the ship security alert messages without delay so as to permit the relevant competent authorities to take appropriate action.

3 Ship security alerts may be addressed to more than one recipient, as designated by the Administration, in order to enhance the resilience of the ship security alert system.

4 The Committee urged once more those SOLAS Contracting Governments that had yet to establish criteria for the delivery of ship security alerts, to do so as a matter of priority.

5 SOLAS regulation XI-2/13.1.3 requires SOLAS Contracting Governments to communicate to the Organization and to make available to Companies and ships the names and contact details of those who have been designated to be available at all times (twenty-four hours a day seven days a week) to receive and act upon ship security alerts.

6 Administrations should ensure that their designated recipients of ship security alerts are capable of processing the information received with the highest priority and taking appropriate actions.

II Testing

1 The Committee agreed that there was a need for ship security alert systems to be subject to testing.

2 However, given the multiplicity of ship security alert systems and the fact that a number of systems in use already had test procedures in place, the Committee decided that it would be impractical to develop a test protocol to cover all systems.

3 The Committee thus agreed that the development of procedures and protocols for testing ship security alert systems were a matter for individual Administrations.

4 Ships, Companies, Administrations and recognized security organizations should ensure that when ship security alert systems are to be tested those concerned are notified so that the testing of the ship security alert system does not inadvertently lead to unintended emergency response actions.

5 When the ship security alert system accidentally transmits, during testing, a ship security alert, ships, Companies, Administrations and recognized security organizations should act expeditiously to ensure that all concerned parties are made aware that the alert is false and that no emergency response action should be taken.