ST. VINCENT AND THE GRENADINES

MARITIME ADMINISTRATION

CIRCULAR N° ISPS 013 – Rev. 2

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

TO: COMPANY SECURITY OFFICERS (CSO) / ALTERNATE COMPANY SECURITY OFFICERS (ALTERNATE CSO), MASTERS, SHIP SECURITY OFFICERS (SSO) AND RECOGNIZED SECURITY ORGANIZATIONS (RSO)

APPLICABLE TO: SHIPS TO WHICH ISPS CODE APPLIES

ENTRY INTO FORCE: DATE OF THIS CIRCULAR

15th April 2025

1. Procedure for testing of SSAS

Pursuant to the requirements of the ISPS Code, the testing of the Ship Security Alert System (SSAS) is applicable for the following categories of vessels engaged in international voyages:

- Passenger ships, including high-speed passenger craft
- Cargo ships**,** including high-speed cargo craft of 500 gross tonnage or more
- Mobile Offshore Drilling Units (MODUs)

The CSO or an alternate CSO of ships carrying out SSAS testing should notify this Administration no **more than 24 hours in advance and no less than 4 hours prior to the test**—by sending a pre-test notification via email to security@svg-marad.com.

The pre-test notification should include the reason of the requirement of testing SSAS (please refer to paragraph 1.1 of this circular).

This is to facilitate the tracking of testing notifications and to avoid unintended emergency response actions.

Please note that other email addresses belonging 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.

Some service providers associated with the shipboard SSAS may routinely transmit reports on vessel location, position, and related data to the CSO and the company. However, this Administration should not be designated as a recipient of such automatic updates.

CSOs, alternate CSOs, SSOs, and Masters shall ensure that internal correspondence or emails are not forwarded or copied to security@svg-marad.com. This designated email should

only be used for pre-test alert notifications, SSAS activation messages, and notification of SSAS faults**.**

The Maritime Safety Committee (MSC) of the International Maritime Organization has adopted the following circulars:

- MSC.1/Circ.1190 – *Guidance on the provision of information for identifying ships when transmitting ship security alerts*
- MSC/Circ.1155 – *Guidance on the message priority and the testing of ship security alert systems*

These documents are annexed to this circular.

1.1 The frequency of SSAS alert test involving the Flag

It has been noted that SSAS tests involving the Flag for some vessels occur very frequently—almost on a weekly basis.

SSAS tests involving the Flag may be conducted on the following occasions only:

- **Vessel transfer to this Flag**
- **Periodical Survey for Cargo Ship Safety Radio Certificate**
- **Third Party Security Verification**
- **Change of Company**
- **Upon the CSO's request (the reason for such a request must be clearly explained in the required pre-test alert notification).**

Upon obtaining agreement from the Flag**,** the vessel may proceed with the SSAS test. The Flag will confirm receipt of the SSAS test message to the CSO or alternate CSO.

1.2 Information in SSAS Test Message to be provided

In the event of a test, the SSAS alert message should include the word "TEST" in the subject line or the message body to avoid triggering an unintended emergency response. The alert message must be restored to its standard operational wording after the test is completed.

Additionally, CSOs, alternate CSOs, SSOs, and Masters are requested to ensure that SSAS onboard is configured to deliver the following information within SSAS messages, in accordance with MSC.1/Circ.1190:

a) Name of the ship
b) IMO Ship Identification Number
c) Call Sign
d) Maritime Mobile Service Identity
e) GNSS position (latitude and longitude) of the ship
f) Date and time of the GNSS position

1.3 Acknowledgement of SSAS Test by this Administration

This Administration will not acknowledge receipt of an SSAS test message unless all of the following conditions, as outlined in this circular, are met:

- The message is sent from a vessel to which the ISPS Code is applicable;
- A proper pre-test notification, including a valid reason for the test, has been submitted in advance; and

- The SSAS test message contains all the information required under paragraph 1.1 of this circular.

1.4 Reset of SSAS Device

It has been observed that, in certain instances, vessels continue to transmit SSAS test messages after testing has been completed.
The CSO or alternate CSO must promptly coordinate with the SSO and the Master to ensure the system is properly reset without delay. This is essential to enable this Administration to effectively monitor the security of its fleet without disruption from repeated SSAS test messages from the same vessel.

2. Procedure in case of transmitting false SSAS message

It has been observed that false SSAS messages transmitted outside working hours or during weekends and holidays were not reported to this Administration and were only addressed on the next working day.

In cases where SSAS equipment is found to be faulty and repeatedly transmits false alerts, the designated CSO must notify this Administration via email at security@svg-marad.com. The CSO must also arrange for shore maintenance staff to rectify the fault without delay. Once the SSAS equipment has been restored to normal operation, this must be reported to the same email address**.**

CSOs, SSOs, and Masters are reminded that in the event of false or erroneous SSAS alerts, immediate action must be taken to inform all concerned parties that the alert is false and no emergency response is needed.

The direct telephone number for SSAS test alerts and SSAS activations is +41 79 447 96 76**.** Please note that this number is also allocated to security emergency purposes**.**

Failure to adhere to the above procedures for testing the SSAS, including the prompt reporting of false alerts to this Administration, will be considered non-compliance and may lead to the imposition of penalties.

Annex to this circular: MSC/Circ.1155 and MSC.1/Circ.1190

Revision history: Rev 2 (completely revised)

Annex B

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7735 7611
Fax: 020 7587 3210

IMO

E

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.

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7587 3152
Fax: 020 7587 3210

IMO

E

Ref. T2-MSS/2.11.1

MSC.1/Circ.1190
30 May 2006

GUIDANCE ON THE PROVISION OF INFORMATION FOR IDENTIFYING SHIPS WHEN TRANSMITTING SHIP SECURITY ALERTS

1 The Maritime Safety Committee (the Committee), at its eighty-first session (10 to 19 May 2006), noted reports that in a number of cases, when the competent authorities designated by Administrations received ship security alerts (SSAs), the information provided to them for identifying the ships[1] transmitting the alert were not adequate and they could not easily identify the ships concerned.

2 The Committee recognized that, if ship security alert systems were to function in an effective and efficient manner so as to provide the security-related benefits for which they were envisioned, there was a need to ensure a harmonized and consistent implementation of the provisions of SOLAS regulation XI-2/6 on Ship security alert systems and of the associated performance standards[2]. As a result the Committee approved the Guidance on the provision of information for identifying ships when transmitting ship security alerts (the Guidance) set out at annex.

3 SOLAS Contracting Governments are invited to bring the Guidance to the attention of owners and of Companies operating ships entitled to fly their flag, of those they have recognized, authorized or approved to provider services in relation to SSAs and of the recognized organizations and the recognized security organizations they have authorized to act on their behalf.

4 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 actions to be taken.

***

1 The term "ship" in this circular refers to the ships which are subject to the provisions of SOLAS chapter XI-2 and of the ISPS Code.

2 Resolution MSC.136(76) on Performance standards for a ship security alert system and resolution MSC.147(77) on Adoption of the Revised performance standards for a ship security alert system.

ANNEX

GUIDANCE ON THE PROVISION OF INFORMATION FOR IDENTIFYING SHIPS WHEN TRANSMITTING SHIP SECURITY ALERTS

INTRODUCTION

1 SOLAS regulation XI-2/6 and the associated performance standards[3] specify that the ship security alert system, when activated, shall, *inter alia*, initiate and transmit a ship-to-shore security alert (SSA) to a competent authority designated by the Administration (the designated recipient) identifying the ship, its location, the date and time of the position and indicating that the security of the ship is under threat or it has been compromised.

2 Administrations have accepted, recognized or approved a variety of equipment and systems to perform the function of the ship security alert system (SSAS) some of which include communication (CSP) and application (ASP) service providers. However, in some cases when the SSA is received by the designated recipient, it does not clearly identify the ship which transmitted the alert.

INFORMATION TO BE PROVIDED TO THE COMPETENT AUTHORITIES

3 When the SSA is delivered to the designated recipient the SSA should include the following information:

.1 Name of ship;
.2 IMO Ship identification number;
.3 Call Sign;
.4 Maritime Mobile Service Identity;
.5 GNSS position (latitude and longitude) of the ship; and
.6 Date and time of the GNSS position.

4 Depending on the equipment, system and arrangements used, the name, the IMO Ship identification number, the Call Sign and the Maritime Mobile Service Identity of the ship may be added to the signal or message transmitted by the shipborne equipment, by the CSP or the ASP, before the SSA is delivered to the designated recipient.

TRANSITIONAL PROVISIONS

5 To bring into line the performance of SSASs, these should be tested as follows:

.1 ships constructed before 1 July 2006, not later than the first survey of the radio installation on or after 1 July 2006; and

.2 ships constructed on or after 1 July 2006, before the ship enters service;

to verify that, when the SSAS is activated, the information specified in paragraph 3 above and the indication that the security of the ship is under threat or it has been compromised are received by the designated recipient. However, if the arrangements established by the Administration are in compliance with paragraph 3 above such additional tests are not required.

---

[3] Resolution MSC.136(76) on Performance standards for a ship security alert system and Resolution MSC.147(77) on Adoption of the Revised performance standards for a ship security alert system.

TRANSFER OF FLAG

6 As from 1 July 2006, upon the transfer of the flag of a ship from another State or another SOLAS Contracting Government, the receiving Administration should test the SSAS to ensure that when the SSAS is activated, the information specified in paragraph 3 above and the indication that the security of the ship is under threat or it has been compromised are received by the designated recipient.

TESTING

7 When testing SSASs, the provisions of paragraphs II.3 and II.4 of the annex to MSC/Circ.1155 on Guidance on the message priority and the testing of ship security alert systems should be observed.

Related provisions: SOLAS regulation XI-2/6, resolutions MSC.136(76) and MSC.147(77), MSC/Circ.1072 and MSC/Circ.1155.