MARITIME AND PORT AUTHORITY OF SINGAPORE
SHIPPING CIRCULAR
NO. 13 of 2024

MPA Shipping Division
460 Alexandra Road
21st Storey mTower
Singapore 119963
http://www.mpa.gov.sg

30 October 2024

Applicable to: Shipowners, ship managers, operators, agents and masters of Singapore-registered ships

TESTING OF THE SHIP SECURITY ALERT SYSTEMS (SSAS) ON SINGAPORE-REGISTERED SHIPS (SRS)

1. This Circular informs shipowners, managers and operators of SRS of the test procedures for SSAS. This Circular supersedes Shipping Circular No. 15 of 2015.

Testing Requirements for SSAS

2. The Maritime Safety Committee (MSC) of the International Maritime Organization had adopted circulars MSC.1/Circ.1190 on *Guidance on the provision of information for identifying ships when transmitting ship security alerts* (**Annex A**) and MSC/Circ.1155 on *Guidance on the message priority and the testing of ship security alert systems* (**Annex B**).

3. Shipowners, managers and operators are requested to ensure that SSAS on board SRS are configured to be capable of delivering the following information within SSAS messages, in accordance with MSC.1/Circ.1190 (paragraph 3 of the Annex):

i. Name of ship;

ii. IMO Ship identification number;

iii. Call Sign;

iv. Maritime Mobile Service Identity;

v. Global Navigation Satellite System (GNSS) position (latitude and longitude) of the ship; and

vi. Date and time of the GNSS position.

4. The procedures for testing of SSAS on board SRS are to be carried out in accordance with MSC/Circ.1155, and as outlined below:

a) The frequency of SSAS alert testing should coincide with the periodical safety radio survey of the ship.

b) Companies and ships carrying out testing of SSAS should notify the Maritime and Port Authority of Singapore (MPA) – not more than 2 days in advance and not less than 4 hours prior to the test – by sending a pre-test notification via email to Shipalert@mpa.gov.sg, to facilitate the tracking of the testing notifications and to avoid unintended emergency response actions.

c) For the testing of SSAS, the test alert message should be configured to contain the word "**TEST**" in the subject heading to avoid unintended emergency response actions. The alert message is to be configured back to the original wordings after the SSAS testing is completed.

d) The Master and the Company Security Officer (CSO) should ensure and verify that SSAS equipment are fully functional, and that test alert messages are sent and received by the correct and relevant addresses, including Shipalert@mpa.gov.sg.

e) In instances where the SSAS equipment is verified to be faulty and continues to transmit repeated false alert messages, the designated CSO shall notify MPA via email at Shipalert@mpa.gov.sg and Shipping@mpa.gov.sg. The CSO shall make relevant arrangements with shore maintenance staff to rectify the technical fault expeditiously. The CSO shall also notify MPA when the SSAS equipment has been restored to normal operation via the same email addresses as listed above.

f) Shipowners, managers and operators shall ensure that any internal correspondences or emails should not be forwarded or copied to Shipalert@mpa.gov.sg. This designated email should only be pre-test alert notifications, SSAS activation messages and notification of SSAS faulty.

g) If shipowners, managers and operators would require a response from MPA on the test of SSAS, a request should be stated explicitly within the pre-test notification email and test alert message. MPA staff will then response to the Master and/or CSO of the vessel upon receipt of the test alert message. If MPA receives multiple/subsequent alerts on the same day, or outside the stipulated test time, normal procedures would be undertaken to validate the nature of the alert with the Master and/or CSO.

5. The testing of SSAS should be undertaken when the ship changes of flag to SRS.

6. The Master and CSO are reminded that in any instances where false or erroneous SSAS alerts are transmitted, expeditious actions should be taken to ensure that all concerned parties are made aware that the alert is false and that no emergency actions are initiated.

7. The direct telephone relating to SSAS test alerts, activation and/or emergencies is (65) 6226 5539.

8. Any queries relating to this shipping circular should be directed to MPA via the following emails Marine@mpa.gov.sg and Shipping@mpa.gov.sg, or telephone (65) 6272 7777.

9. Do subscribe to our Telegram channel – t.me/MPASingapore to receive the latest updates.

CHEAH AUN AUN
DIRECTOR OF MARINE
MARITIME AND PORT AUTHORITY OF SINGAPORE

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.

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.

_____