REPUBLIC OF THE UNION OF MYANMAR
MINISTRY OF TRANSPORT
DEPARTMENT OF MARINE ADMINISTRATION

NO.363/421, CORNER OF MERCHANT & THEIN BYU ROAD,
BOTATAUNG TOWNSHIP, YANGON, MYANMAR

P.O BOX 194, Fax: +95 1 397641, E-mail: dgdma@myanmar.com.mm

Date : 7th October 2014

Directive(10/2014)

Ship Security Alert System (SSAS)

Applicable to: All Ship - owners, Ship Operators, Flag State Surveyors, Recognized Organizations, Masters and Officers of Myanmar Flagged Ships.

Reference :

(a) **SOLAS 1974, as amended Reg: XI-2 / 6**
(b) **Guide to Maritime Security and the ISPS Code**
(c) **IMO Res MSC.136(76)**
(d) **IMO Res MSC.147(77)**
(e) **IMO Res MSC. 1072**
(f) **IMO Res MSC/Circ.1109/Rev.1**
(g) **IMO Res MSC/Circ.1155**
(h) **IMO Res MSC.1/Circ.1190**
(i) **Shipping circular No.3/2004 and 1/2006 in accordance with SOLAS Chapter XI-2/6.2.1**

1. The Department of Marine Administration circulates this directive in the exercise of the power of Section 294(B), paragraph (b) of Myanmar Merchant Shipping Act 1923, as amended.

2. This directive applies to all Myanmar flagged ships engaged on International voyages complying with requirements of the International Convention for Safety of Life at Sea 1974, as amended.

3. Shipping Companies and Myanmar flagged ships engaged on International voyages shall comply with Ship Security Alert System in accordance with SOLAS 1974, as amended Reg: XI-2 / 6 and above references.

4. The Guidance for the Ship Security Alert System is set out by Department of Marine Administration to fulfill the relevant requirements of the above-mentioned references.

Maung Maung Oo
Director General
Department of Marine Administration

Department of Marine Administration
Ministry of Transport and Communications
Republic of the Union of Myanmar

GUIDANCE FOR THE SHIP SECURITY ALERT SYSTEM

2014

DMA

Introduction

1. This Guidance for the Ship Security Alert System applies to Shipping Companies andtheir employed on Myanmar flagged ships.

2. The requirement of a Ship Security Alert System may be complied with by using the radio installation fitted for compliance with the requirements of SOLAS, Chapter IV, provided all requirements of this regulation are complied with.

3. The Ship Security Alert System is provided to a ship for the purpose of transmitting asecurity alert to the shore to indicate to a competent authority that the security of the ship is under threat or has been compromised.

4. This Guidance for the Ship Security Alert System isset out on 7thOctober 2014 according to the directive 10/2014 in the e xercise of the power of Section 294 (B), paragraph (b) of Myanmar Merchant Shipping Act 1923, as amended.

Guidance for the Ship Security Alert System

CONTENTS

Guidance for the Ship Security Alert System

PART A

GENERAL

1. Application

This guidance applies to the approval and inspection of Ship Security Alert Systems fitted on ships engaged on international voyages according to the requirements specified in Chapter XI-2 of the International Convention for the Safety of Life at Sea 197, as amended.

2. Definitions

2.1 Ship Security Alert System (SSAS) provides the means by which a ship can transmit a security alert to a competent authority on shore, indicating that the security of the ship is under threat or has been compromised.

3. Ship Security Alert Systems

3.1 A Ship Security Alert System (SSAS) transmits a covert alarm to one or more competent authorities ashore indicating that the security of the ship is under threat or has been compromised. Ship security alerts can be activated in the event of any serious security incident, including acts of piracy and armed robbery against the ship.

3.2 Guidance on installation and operation of SSASs on ships is in paragraphs 4.13 to 4.22. These details need not be included in SSPs but can be included in a separate document known to the master, SSO or other senior shipboard personnel selected by the Company.

3.3 Administrations designate one or more competent authorities ashore to receive ship security alerts from their SOLAS ships. Any designated competent authority should be able to obtain a covert verification from the ship and alert the country's security forces responsible for initiating the security response to acts of violence against ships.

3.4 Administrations have to establish an effective means of communication between their competent authorities and the security force responsible for the response.

3.5 Many Administrations have designated Company Security Officers (CSOs) and a selected Maritime Rescue Co-ordination Centre (MRCC), or equivalent agency, as their competent authorities. Protocols have to be in place to ensure immediate communication between CSOs receiving a ship security alert and the selected competent authority (which is the point of contact with the responding security force). CSOs are often in the best position to seek verification of alerts from their ships. Covert verification can be achieved by pre-arranged exchanges of messages.

3.6 Other Administrations have designated a MRCC as their sole competent authority for the receipt of ship security alerts. In such cases, the MRCC should establish procedures for verifying individual ship security alerts.

3.7 Unless directed by the Administration or security force, a competent authority who receives a ship security alert should not overtly acknowledge its receipt to the ship.

3.8 Administrations should provide guidance to competent authorities on the procedures to be followed on the:

.1 prioritization of ship security alerts;

.2 distinction between covert and overt alarms;

.3 receipt of false security alerts and distress/security double alerts; and

.4 testingship securityalert systems and associated communication procedures.

3.9 IMO has requested that information be provided on the receipt of false security alerts and distress/ security double alerts.

3.10 Administrations should ensure that ships flying their flag test ship security systems and associated communication procedures on a regular basis. When doing so, it should be made clear that it is a TEST alert.

3.11 In consultation with their responding security forces, Administrations should develop protocols on notifying MRCCs in the vicinity of the ship, their Governments, and the Administrations or response organizations in adjacent countries of the receipt of an alert.

3.12 Upon receiving notification of a security alert from a ship entitled to fly its flag, the Administration must immediately notify the State(s) in the vicinity of which the ship is presently operating. If a security alert is received from a ship that is not entitled to fly its flag, that Contracting Government must immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

3.13 All ships are required to be provided with a Ship Security Alert System (SSAS) as described in paragraphs 4.1 to 4.12 Its intent is to send a covert signal or message from a ship that will not be obvious to anyone on the ship who is unaware of the alert mechanism.

3.14 When activated, the SSAS must:

.1 initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration, which in these circumstances may include the shipping company, identifying the ship and its location, and indicating that the security of the ship is under threat or has been compromised;

.2 not send the alert to any other ships;

.3 not raise any alarm on board the ship; and

.4 continue the alert until deactivated and/or reset.

3.15 The competent authority should be able to receive SSAS alerts on a 24/7 basis.

3.16 The SSAS must:

.1 be capable of being activated from the navigation bridge and in at least one other location;
.2 conform to performance standards not inferior to those adopted by IMO; and
.3 have its activation points designed so as to prevent the inadvertent initiation of an alert.

3.17 When an SSAS alert is received by the competent authority, either directlyor via a service provider, it should include the following information:

.1 name of ship;
.2 IMO ship identification number;
.3 call sign;
.4 Maritime Mobile Service Identity (which is a series of 9 digits sent over a radio-frequency channel to provide a unique identifier used to call ships automatically);
.5 GNSS position of the ship; and
.6 date and time of the GNSS position.

3.18 The requirement for an SSAS may be met by using radio installations that have been approved by the Administration.

3.19 The competent authority is responsible for ascertaining whether a security alert is real or false.

3.20 The SSP must include the following, which Administrations may require to be kept in a document separate from the SSP to avoid compromising its confidentiality:

.1 the identification of the SSAS activation points; and
.2 procedures to be used, including testing, activation, deactivation and resetting to limit false alerts.

3.21 A master may use an overt alarm (i.e., one such as a VHF broadcast, which makes no attempt to deny knowledge of its activation) in addition to a covert alarm of discouraging a security threat from becoming a security incident.

3.22 Experience to date of ship operators in establishing SSASs reveals examples of:

.1 procedures being included in SSPs using a standard template;
.2 the handling of false security alerts being included as a procedure;

.3 testing being performed at least annually;

.4 all concerned parties being notified by the shipping company when an SSAS is to be tested, so as to avoid any unintended emergency response actions.

.5 When an SSAS accidentally transmits in testing, the ship immediately notifying the Shipping company or competent authority (if it is not the shipping company), so that all concerned parties can be made aware that the alert is false and that no emergency response action should be taken;

.6 a checklist being used when testing; and

.7 providing for an alternative power source.

3.23 The system is to have at least two manually operated call points.

The manually operated call points (buttons) are to be designed such that any inadvertent operation will be prevented and that the operator can start the system without removing any seal or lid/cover.

3.24 When starting (activating) an alarm, no adjustment is allowed on involved devices, such as choosing frequency, setting working mode or selecting menu, nor is any (other) alarm to be activated thereby on board.

3.25 The alarm message of the security alert system is to include the ship's name, IMO identification number, call sign, maritime mobile services identity, ship GNSS position signals (including longitude and latitude) and time of GNSS ship position signals (date/month/year and time).

3.26 SSAS alarm is not to be transmitted through GMDSS distress alarm procedure and is only to be sent to coast station without notification to the ship.

3.27 Once activated, SSAS alarm is to keep transmitting the ship security alert before being turned off and/or reset.

3.28 SSAS is to be capable of testing and indicating that the transmitted message is for test purpose.

3.29 SSAS is to be fitted with power switch, reset button, power indicating light, alarm transmitting light, failure indicating light on the main controlling unit.

3.30 In addition to the main source of electrical power of the ship, an optional source of electrical power is to be available for SSAS, which can be either a power source other than the main one, or an integrated power source of the equipment. Furthermore, the two types of power sources are to be capable of being switched from one to another.

3.31 The software of SSAS is to be designed for the above requirements and in addition, for completeness, independence, reliability and confidentiality Such software is also to be capable of being upgraded and functionally expanded so far as possible.

3.32 The procedure for testing the SSAS for Myanmar Flagged ships, should be in accordance with MSC/Circ.1155. The frequency of SSAS alert testing involving Department of Marine Administration should not exceed more than one a year and should coincide with the annual safety radio survey.

PART B

RECOMMENDATION ON PERFORMANCE STANDARDS FOR A SHIP SECURITY ALERT SYSTEM

1. Introduction

1.1 The Ship Security Alert System is provided to a ship for the purpose of transmitting a security alert to the shore to indicate to a competent authority that the security of the ship is under threat or has been compromised. It comprises a minimum of two activation points, one of which is on the navigation bridge. These initiate the transmission of a ship security alert. The system is intended to allow a covert activation to be made which alerts the competent authority ashore and does not raise an alarm on board ship nor alert other ships.

1.2 As required by its Administration, the competent authority receiving the alert notifies the authority responsible for maritime security within its Administration, the Coastal State(s) in whose vicinity the ship is presently operating, or other Contracting Governments.

1.3 The procedures for the use of the ship security alert system and the location of the activation points are given in the ship security plan agreed by the Administration.

1.4 The Ship Security Alert System may utilise the radio installation provided for compliance with chapter IV of the SOLAS Convention, other radio systems provided for general communications or dedicated radio systems.

2. General

2.1 In addition to complying with the general requirements set out in resolution A.694 (17) the ship security alert system should comply with the following performance standards.

2.2 The radio system used for the ship security alert systems should comply with relevant international standards.

3. Power supply

Where the Ship Security Alert System is powered from the ship’s main source of electrical power, it should, in addition, be possible to operate the system from another appropriate source of power.

4. Activation points

Activation points should be capable of being used on the navigation bridge and in other locations. They should be protected against inadvertent operation. It should not be necessary for the user to remove seals or to break any lid or cover in order to operate any control.

5. Operation

5.1 The activation points should operate a radio system such that transmission of the security alert does not require any adjustment of the radio system, i.e. tuning of channels, setting of modes or menu options. Operation of the activation point should not cause any alarm or indication to be raised on the ship.

5.2 The operation of the Ship Security Alert System should not impair the functionality of the GMDSS installation.

6. Transmission of security alerts

6.1 In all cases, transmission initiated by security alert system activation points should include a unique code/identifier indicating that the alert has not been generated in accordance with GMDSS distress procedures. The transmission should include the ship identity and current position. The transmission should be addressed to a shore station and should not be addressed to ship stations.

6.2 The Ship Security Alert System, when activated, should continue the ship security alert until deactivated and/or reset.

7. Testing

7.1 The Ship Security Alert System should be capable of being tested.

PART C

FALSE SECURITY ALERTS AND DISTRESS/SECURITY DOUBLE ALERTS

1. SOLAS regulation XI-2/6 requires ships to be fitted with a SSAS which, when activated, shall initiate and transmit a ship-to-shore security alert (security alert) to a competent authority designated by the Administration, indicating that the security of the ship is under threat or it has been compromised. The requirement for the carriage of SSAS, which is a covert system, is additional to the requirement to be provided with radio communication equipment capable of initiating and transmitting distress alerts and piracy attack alarms, both of which are overt systems. MSC/Circ.1110, which provides guidance on Matters related to SOLAS regulations XI-2/6 and XI-2/7, is also relevant.

2. Experience with false distress alerts gained since the introduction of GMDSS and a study of the information submitted in relation to "false security alerts" indicate that a ship may transmit a "false security alert" either as a result of technical failure of the SSAS or due to inadvertent activation of the system. In either case, since SOLAS regulation XI-2/6.2.3 provides that SSAS, when activated, shall not raise any alarm on board the ship, shipboard personnel may be unaware, or unable to establish, whether a security alert is in fact being transmitted.

3. The Committee, at its seventy-eighth session, was therefore requested to advise what action should be taken between the time a security alert is first received ashore and the time that the competent authorities initiate action to address the security alert, bearing in mind that there is a need to determine whether the security alert received ashore is a genuine or a false one.

4. The Committee was also requested to consider what action should be taken in the event of a ship transmitting a distress alert and a security alert (distress/security double alert), either simultaneously or one after the other. In view of the fact that a security incident may lead to a distress situation or a distress situation may be followed by a security incident; and since all ships are capable of transmitting both alerts, simultaneously or in tandem; the competent authorities ashore need to assess the situation so as to determine and prioritize the response to be provided.

5. The Committee, bearing in mind the need to identify the nature and extent of the aspects involved, decided, at its seventy-ninth session, to consider these proposals further at a future session in the light of the actual experience gained in the interim from the use of SSAS.

PART D

GUIDANCE ON PROVISION OF THE SHIP SECURITY ALERT SYSTEM

1. Regulation 6 of SOLAS chapter XI-2 requires ships to be provided with a Ship Security Alert System. Section A/9 of the International Ship and Port Facility Security (ISPS) Code requires ships to carry a ship security plan. Performance standards for ship security alert systems are given in resolution MSC. 147(77). This Circular gives guidance on the design of ship security alert systems provided to comply with the SOLAS regulation.

2. The intent of the Ship Security Alert System is to send a covert signal or message from a ship which will not be obvious to anyone on the ship who is not aware of the alert mechanism. It is of use therefore in circumstances where a ship wishes to inform a person ashore of a problem with a minimum number of the persons onboard aware of the action. The procedures for the security alert are agreed with the ship's Administration as part of the ship security plan and ideally should be individual to the ship. It is not intended that the ship security alert procedures should be to an internationally agreed standard or conform to any particular for all ships.

3. Possible methods of achieving the alert are as follows:

.1 a system may employ proprietary tracking equipment provided by traffic service providers. The ship then carries a concealed equipment box working over a satellite system on its upper deck which transmits a positionreport at, typically, 6-hourly intervals. Interruption of power to the equipment or arming of the equipment by means of sensors or manual buttons causes the equipment to transmit a different format of position report. The tracking service providers monitor the transmission reports and inform the Company when the transmission format changes;

.2 a system may utilize modifications of GMDSS equipment. Some GMDSS equipment is not very suitable for modification as it is optimized for "all station" calling and may involve manual setting of frequencies etc and provides confirmation on the ship of messages sent. In these types of systems the ship security alert contains identifiers to ensure that it is not possible to confuse it with a GMDSS distress, urgency or safety alert; and

.3 a system may utilise the exchange of messages containing key words between a ship and, typically, the Company. These messages may be by speech or data communications. Ship equipment which may be used includes cellular phones in coastal areas and satellite services away from coastal areas. It may be possible to use GMDSS VHF/MF/HF equipment in areas where there are coastal facilities for receiving addressed calls.

This list is not intended as exhaustive and is not intended to inhibit future developments.

.4 The Ship Security Alert System requires two activation points, one of which should be on the bridge. These will typically be fixed or portable telephone handsets, fixed or portable keypads or fixed or portable buttons.

.5 Measures should be incorporated in the activation points to avoid their inadvertent operation and the generation of false alerts.

PART E

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

I Message priority

1. The Committee, being a ware 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 ships security alert messages without delay so a stop permit here levant competent authorities to take appropriate action.

3. Ship Security Alerts may be a ddresed to more than one recipient, as designated by the Administration, in order to enhance there salience of the ships security alert system.

4. The Committee urged once more those SOLAS Contracting Governments that had yet toes table is hcriteria 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 name sand contacted tails 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 system sand the fact that a number of systems in use already had test procedure sin place, the Committee decided that it would be impractical to develop attest 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 in advertently 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 respon section should be taken.

PART F

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 specify that the ship security alert system, when activated, shall, *interalia*, 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. Administration shave 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 BEPROVIDED TO THE COMPETENT AUTHORITIES

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

(i) Name of ship;
(ii) IMO Ship identification number;
(iii) Call Sign;
(iv) Maritime Mobile Service Identity;
(v) GNSS position (latitudeand longitude) of the ship;
and DateandtimeoftheGNSSposition.

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 ship borne equipment, by the CSP or the ASP, before the SSA is delivered to the designated recipient.

TRANSITION ALPROVISIONS

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.

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.