#### **Commonwealth of Dominica**



### Office of the Maritime Administrator

TO: ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS

OF MERCHANT SHIPS, MOBILE OFFSHORE DRILLING UNITS

AND RECOGNIZED ORGANIZATIONS

SHIP SECURITY ALERT SYSTEM GUIDELINES **SUBJECT:** 

**REFERENCE:** a) SOLAS Chapter XI-2, Regulation 6

b) IMO Resolution MSC.136(76)

c) Marine Safety Circular no. CD-MSC 12-03

**PURPOSE:** The purpose of this Safety Circular is to provide guidance to the

> Owners and Operators of Dominica vessels regarding the installation, programming and verification of the ship security alert systems fitted on board in accordance with SOLAS regulation XI-2/6 and performing to the standards prescribed in IMO Resolution MSC.136(76) and Dominica Marine Safety Circular no. CD-MSC 12-

03.

APPLICABILITY: The following types of the Commonwealth of Dominica flag vessels engaged on international voyages:

- passenger ships, including high-speed passenger craft;

- cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and
- mobile offshore drilling units.

## **REQUIREMENTS:**

#### 1 **Programming**

- 1.1 At a minimum the ship security alert system (SSAS) message should provide:
  - vessel's name
  - IMO number
  - call sign, position
  - course and speed
  - date and time (UTC) of message.

1.2 Additional information such a the name and contact phone number for the Company Security Officer (CSO) may be included if the SSAS is capable of such programming but this additional information is not required.

## **2** Competent Authority

The competent authority for Commonwealth of Dominica is the Office of the Deputy Maritime Administrator, Maritime Affairs, Attn: Deputy Maritime Administrator.

#### 3 Destination

- 3.1 For Dominica flag vessels the ship security alert shall be sent directly to both the Company and the Administration. The SSAS should be programmed to send an alert message to: security@dominica-registry.com.
- 3.2 If the Company has authorized a third party service provider to receive the SSAS messages on behalf of the Company, this Administration (<a href="registry.com">registry.com</a>) shall be provided with the name and contact information for the service provider of the SSAS and coverage of their ships.

## 4 Testing

- 4.1 The Administration requires a test message as soon as the SSAS has been activated and at least once a year thereafter.
- 4.2 During testing of the system, the test message should contain the words: "TEST" in order to identify it as such and avoid the need for additional communication between the CSO and the Administration. If the system is not capable of inserting the word "TEST" into the alert message, then the CSO must send an advance e-mail to the Administration (security@dominica-registry.com) advising the Administration that the system will be tested.

#### 5 Initial SSAS Verification

- 5.1 The onboard installation and operation of the SSAS must be verified as follows:
  - .1 ships constructed on or after 1 July 2004 not later than the first security verification after 1 July 2004;
  - .2 passenger ships, including high-speed passenger craft, constructed before 1 July 2004 not later than the first survey of the radio installation or the first security verification after 1 July 2004, whichever comes later;

- .3 oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high-speed craft, of 500 gross tonnage and upwards constructed before 1 July 2004 not later than the first survey of the radio installation or the first security verification after 1 July 2004, whichever comes later; and
- .4 other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before 1 July 2004 not later than the first survey of the radio installation after 1 July 2006.
- 5.2 The onboard verification of SSAS shall be performed by a security auditor with the Dominica RSO that performed the initial security verification of the vessel on behalf of Dominica or that is also the RO for the purposes of statutory certification of that vessel. The SSAS equipment and its operation are confidential. The number of individuals involved in review and verification process, and who have knowledge of the location of the activation buttons should be limited.

# 5.3 Verification procedure:

- .1 <u>Ship Security Plan amendments</u>: Only those pages in the SSP that relate to the SSAS must be amended. The SSP including the amended pages and the updated record of changes shall be submitted to: <a href="mailto:registration@dominica-registry.com">registry.com</a> for review and approval in advance of the onboard verification.
- .2 Sending a test message: Prior to having the installation verified by an auditor, the vessel shall send an SSAS test message to the Administration in order to verify the proper performance of the system. Confirmation of receipt of the SSAS message will be sent by e-mail to the CSO. The CSO should provide a copy of the confirmation message to the ship's Master, so it can be available to the auditor who verifies the SSAS installation.
- Onboard verification by the auditor: During the SSAS verification, the security auditor will evaluate the procedures outlined in the SSP, interview the Master and SSO on their knowledge of the procedures, verify the installation and programming of the SSAS, and endorse the International Ship Security Certificate (ISSC) in the space marked "Additional verification". A copy of the endorsed certificate shall be forwarded to the Administration for issuance of a final ISSC valid for the period of full five (5) years since the date of initial security verification. In order for vessel Owners to not incur additional costs, no special attendance is required. The SSAS verification can take place in conjunction with another scheduled inspection, audit or survey provided:
  - the inspector or surveyor is also an authorized security auditor, and
  - the onboard verification takes place no later than by the deadlines prescribed in section 5.1 above for respective vessels.

# 6 SSAS false alert message

Should an SSAS message be sent that is not a test or an actual alert, the CSO shall immediately confirm that the SSAS message was sent in error. The CSO will then inform all concerned parties and the Administration that the alert is false and that no emergency response action should be taken.