CCS 通 函

Circular

中国船级社
（2012 年）通告第 55 号总第 217 号
2012 年 5 月 29 日（共 13 页）

发：总部相关处室、各分社/办事处并转船公司

船舶保安警报系统(SSAS)
--转发马绍尔海事主管机关海事通告 No.2-011-18,Rev.2/12

马绍尔海事主管机关近期下发 No.2-011-18，Rev.2/12 海事通告，向船东、经营人、商船的船长和高级船员以及认可组织就船舶上配备的 SSAS 的功能和马绍尔的国家规定进行了说明。它为船东、船舶经营人和保安认可组织（RSOs）提供了管理信息，同时为制订满足规则 XI-2/6 要求的体系提供了技术指导。本通告替代了 Rev. 8/06，修正了 2.4 节中的邮件地址，增加了 12.0 节-船舶保安警报系统。我社审核员在代表马绍尔海事主管机关进行相关检查和审核时应予以关注，并提醒相关船舶和公司遵照执行。

适用范围:

规则 XI-2/6 适用于从事国际航行的以下类型的船舶:

(a) 客船，包括高速客船;

(b) 货船，包括500总吨或以上的高速货船；以及

(c) 第IX/1章中定义的非就位状态的机械式推进海上移动式钻井平台。

要求:

1.0 <u>执行</u>

1.1 所有上述种类的船舶须按照下面要求配备SSAS:

.1 在2004年7月1日或以后建造的船舶;

.2 在2004年7月1号以前建造的客船，包括高速客船，不迟于2004年7月1日以后的第一次无线电装置检验之前;

.3 在2004年7月1号之前建造的500总吨及以上的油船、化学品液货船、气体运

输船、散货船和高速货船，不迟于2004年7月1号之后的第一次无线电装置检验之前；以及

.4 2004年7月1日以前建造的500总吨及以上的其它货船和海上移动式钻井平台，不迟于2006年7月1日以后的第一次无线电装置检验之前。

1.2 关于符合MSC/Circ.1190中附加功能的要求，上述种类的船舶须按下面要求配备符合要求的SSAS或者按照如下升级SSAS:

.1 在2006年7月1日或之后建造的船舶，符合要求；

.2 在2006年7月1号之前建造的客船包括高速客船，不迟于2006年7月1号以后的第一次无线电装置检验，升级；

.3 在2006年7月1号之前建造的500总吨及以上的油船、化学品液货船、气体运输船、散货船和高速货船，不迟于2006年7月1号之后的第一次无线电装置检验，升级；以及

.4 2006年7月1日以前建造的500总吨及以上的其他货船和海上移动式钻井平台，不迟于2006年7月1日以后的第一次无线电装置检验、升级。

1.3 SSAS启动的所有船舶保安警报（SSAs）须发送至RMI海事主管机关（“主管机关”）和公司保安员（CSO）。

1.4 SOLAS第XI-2章第6条要求，所有船舶须安装SSAS，在紧急情况下启动SSAS时，系统会传送保安警报至指定的主管机关。SOLAS第XI-2章中要求的船舶保安警报系统，并不被认为是无线电设备，因此没有包括在无线电安全检验中，并且不会受无线电安全证书影响。但是，船舶保安警报系统中存在的任何缺陷都是对ISPS规则和ISM规则潜在的缺陷。

2.0 <u>适任主管机关</u>

2.1 适任主管机关是指接收到来自船舶的警报并将其发送至主管机关和CSO的机构。适任主管机关必须证明它可以在任何时间接收到来自船舶的SSA并立即进行转发。

2.2 结合SSAS功能提供资产追踪服务的供应商，比如Globe Wireless、Purple Finder、Trans as、Iridium等，也可以担当主管机关的责任。

2.3 希望为悬挂RMI旗的船舶提供SSAS服务的公司或组织，应向主管机关提供一份将要安装或改进设备的详细说明以及一份作为适任主管机关的协调通信计划。系统的详细内容应包括：设备、覆盖区域和通信计划，并也应递交至RSO 接受审查。

2.4 希望直接发送 SSAs 至主管机关和 CSO 的公司或希望作为适任主管机关来发

送SSAs至主管机关和CSO的机构，应确认按照下面的地址向带有无线电服务的区域主管机关提交SSAs的技术安排：

Marshall Islands Maritime and Corporate Administrators

11495 Commerce Park Drive

Reston, Virginia 20191-1506

USA Tel: +1-703-620-4880

Fax: +1-703-476-8522

Email: nsantram@register-iri.com

2.5 在安装过程中，主管机关将根据申请向CSO提供SSA邮件地址和电话号码。

3.0 船舶保安计划

3.1 要求SOLAS船舶在其保安计划中记录SSASs。主管机关的RSO将结合他们对船舶保安计划的审查对船舶的SSAS设备和程序进行审查。第二处启动点的位置应该在船舶保安计划中详细说明并对此进行保密。但是，为了避免泄露船舶警报系统目标，主管机关建议此信息应保存在只有船长、SSO和其它船上的高级管理人员知道的另外的文件中。

3.2 如果船舶已经有一个经批准的保安计划，该计划必须进行修订以说明SSAS的情况，并且相关的部分必须放在船上以备接受在初次安装之后的符合性审核中的审查和批准。这应该包括为符合这些规定而在特定船舶上安装任何设备的记录。

3.3 必要时，除其他事项外，船舶的初次国际船舶保安证书的持续有效取决于，不管船舶保安系统何时进行中间或换新审核，船舶在适用的无线电安全检验实施日期前安装了有效的SSAS。

3.4 在不要求配备SSAS的船上安装的SSAS系统，也要满足这些总体的要求。

4.0 系统要求

4.1 经MSC.147(77)修订的IMO决议MSC.136(76)中给出了SSASs的性能标准。MSC/Circ.1072 和MSC/Circ.1155对提供符合SOLAS规则的SSASs的设计和功能要求给出了更进一步的指导。

4.2 SSAS可能是现有的无线电装置的一部分，但不能影响该设备的正常功能。如果SSAS使用了任何新的或改装的现有的无线电传送设备，那么供应商必须认证该设备。生产商必须检查任何新的电子设备，以符合IEC60945的相关要求，这是对所有的设备类型要求。

4.3 如果SSAS使用了船舶的主电源，则应提供一个适当的备用电源。这可以是一个现用的备用可替换电源或专用电池组。对于这个系统来说，可以考虑使用不间断电源（UPS）或类似的以船舶的主电源作为可替换动力源。

5.0 应用

5.1 保安警报不应和船舶进行的任何其它例行报告一起传送。信息传输应自动生成，不需要操作员除激活系统以外的任何输入。移动电话不能作为符合此要求的自动设备。为符合MSC/Circ.1190 和RMI要求，主管机关最终接收到的信息必须包括:

(a) 船舶名称;
(b) IMO船舶编号;
(c) 船舶呼号;
(d) 海上移动业务编号;
(e) 日期和时间;
(f) 位置;
(g) 航线和速度;
(h) CSO 名称和 24/7 电话号码;
(i) CSO替代人员名称和 24/7 电话号码; 以及
(j) 陈述SSAS已被激活和表明船舶正处于威胁中或已受危害的信息。

5.2 如果使用资产追踪服务，将会在信息中提供对监控代理的活动超链接。超链接的操作应该是自动地或由主管机关使用统一用户帐号和指派给主管机关的密码进行操作。当收到保安警报信息时，该信息可以使主管机关更快联系到最近的沿岸国指定的主管机关以及CSO。

5.3 保安警报必须能够在船舶即将航行的航线的任何一点上都能传送至主管机关和CSO。该警报不应作为一般遇险信号发送。它应该单独地直接发往主管机关和CSO。 因为事先经过授权，它可以通过适任主管机关完成。

5.4 视频传输，比如经加密的无线电传输，要进行仔细地评估，并且依据船舶航线决定是否可以接受。

6.0 初次安装和型式认可

6.1 要求船东在安装SSAS之前通知RSO.

6.2 依据安装和操作类型，有两（2）种有效的船舶保安警报系统，一般称为船舶保安警报系统（SSAS）和自给式SSAS（SSAS-SC）。公司应了解其中的差异和他们的船舶适合安装哪种型号，以便于提供适当的软件和界面来确保主管机关在上面5.1部分中列出的所有要求信息的最终接收。

6.3 主管机关不会为SSASs 或 SSAS-SCs进行任何正式的型式认可。主管机关的RSO在船舶保安计划审批中将会审查和批准船舶的具体系统。可以在主管机关的网站 www.register-iri.com 上的海事安全通告中有RSOs联系信息的清单。

7.0 “SSAS”

7.1 这是一个要求有接口，和/或依赖于源自SOLAS第 IV 章和第V章中要求的无线电或导航设备的输入，以满足SOLAS 第XI-2/6条规定的性能标准。SSAS是SOLAS第XI-2章中的要求，并不受无线电安全证书影响。

7.2 在所有情况下，负责签发无线电安全证书的RO须负责安排经认可的无线电工程师进行SSAS的初次安装检查和试验。船上需保存证明符合SOLAS 规则XI-2/6 第2-4款和MSC/Circ.1190的无线电工程师报告的副本，供RSO在下一次定期审核时使用。“SSAS的安装符合SOLAS 第XI-2/6条 第2-4款和 MSC/Circ.1190”之类的说明，应写入经批准的GMDSS无线电装置记录中。应当注意，货船无线电安全证书设备记录“R”中不应包括SSAS的详情。SSAS装置应接受经认可的无线电工程师的年度检查。

8.0 SSAS-SC

8.1 此系统不要求接口，和/或依赖于源自SOLAS第 IV 章和第V章中要求的无线电或航行设备的输入，以满足SOLAS第XI-2/6条规定的性能标准。但是，为使系统符合MSC/Circ.1190要求的附加信息，仍有必要对现有装置进行软件修订。该设备在船上安装和启用，并不要求进行初次安装检验。SSO可以对SSAS-SC进行检查和报告。

9.0 船上审核

9.1 在SSAS或 SSAS-SC初次安装之后的下一个船舶的ISPS审核中，审核员须审查和批准SSP中相关的条款，按照ISPS规则A/9.4.17 到 A/9.4.18的要求，现场验证一个完整的保安警报测试以及审核SSAS或SSAS-SC的操作要求，并在SSAS审查中，检查经批准的GMDSS无线电装置记录、符合声明或等效文件。

9.2 在随后的每个ISPS审核中，审核员须检查ISPS规则A/10.1.10中规定的SSAS或SSAS-SC的活动报告，现场验证一个完整的保安警报测试以及审核操作要求，并在SSAS审查中，检查经批准的GMDSS无线电装置的记录、符合声明或等效文件。

9.3 一个“完整的”保安警报试验须要求发送测试信息至 CSO 和主管机关。

10.0 测试

10.1 在SSAS或SSAS-SC的初次安装之后，公司的责任有:

- 确保系统进行测试和维护，以符合经批准的SSP的操作要求；以及
- 在船上保存ISPS规则 A/10.1.10中要求的系统记录。

10.2 系统须能进行测试来核实是否正确操作。测试应包括整体的警报系统，从启动到CSO收到警报。

10.3 系统还可以按要求在港口国控制检查员面前进行测试，但仅能从驾驶室位置开始，并且要适当地提前告知CSO和主管机关。

10.4 应在船舶保安计划中或在仅供船长、SSO或其他受委托的船舶高级船员察看的单独文件中列出测试的程序，包括适当的主管机关的电话号码和保安邮件地址。

10.5 在进行测试之前，如果需发送信息至主管机关，要求将测试提前通知主管机关。针对这些要求主管机关核实收到信息的测试，应和主管机关提前做好安排。

10.6 CSO应注意，主管机关应仅在下述情况下接受警报测试:

- SSAS 或SSAS-SC系统安装;

- ISSC证书的中间审核/检验；
- ISSC证书换新审核/检验。

10.7 测试信息应标有“测试”字样。

10.8 测试应在官方航海日志中正确记录。

11.0 启动

11.1 保安警报的启动应仅需一项行动，而不包括打开防护覆盖层。通常至少要有两个启动点。一个必须位于驾驶台，其它点位中的至少一个应位于通常可以立即到达的地方，比如机舱控制中心、船长室、海员休息室等。启动点一定不能在开始报警之后再进行警报解除，并且一定要防止无意中触发报警。启动点不应用封条或盖子这种需要打破才能启动警报的物品来进行保护。一个破了的封条就可以表明警报已被启动。可以使用无警报状态指示的弹簧盖子或类似的设备。

11.2 警报一旦启动，系统应以不少于30分钟一次的频率持续发送保安警报，直到CSO确认警报状况并且CSO批准重新设定或解除警报。应有一个保密程序来正确核实警报状态和系统的重设和解除。除非CSO可以对此进行远程操控，船舶应启动系统失效。

11.3 当主管机关接收到状态无法确认SSA时，应立即告知当前进行此操作的船舶附近的沿岸国。CSO要和主管机关一起立即核实每个SSA状态，避免错误警报，这点是非常有必要的。

12.0 船舶保安报告系统(SSRS)

授权并强烈建议船东订制SSRS，因为它可以实现船舶运营和海军行动之间的实时联系，因此可以提升现有SSAS抗击海盗的效果。详细内容参考MN 2-011-31。

****

附件：Marshall Island Marine Notice No.2-011-18, Rev.2/12, 共7页

中文翻译如有歧义，以马绍尔主管机关海事通告原文为主。本通告在实施过程中如有任何疑问，请与总 部：**认证处** 联系。

REPUBLIC OF THE MARSHALL ISLANDS

OFFICE OF THE MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-18

Rev. 2/12

TO: **ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS, AND RECOGNIZED ORGANIZATIONS**

SUBJECT: **Ship Security Alert System (SSAS).**

References:
- **(a) Safety of Life at Sea (SOLAS) 1974, Chapter XI-2, Reg. 6**
- **(b) IMO Resolution MSC.136(76), as amended by MSC.147(77)**
- **(c) IMO MSC/Circ.1072**
- **(d) IMO MSC/Circ.1155**
- **(e) IMO MSC/Circ.1190**
- **(f) Marine Notice 2-011-31**

PURPOSE:

This Notice explains the functioning and National requirements of the SSAS as it applies to Republic of the Marshall Islands (RMI) flagged vessels. It provides administrative information for vessel owners, operators and Recognized Security Organizations (RSOs) as well as technical guidelines for developing systems to meet requirements of Regulation XI-2/6. This Notice supersedes Rev. 8/06 and reflects the change in the email address in section 2.4 and the addition of section 12.0, Ship Security Reporting System.

APPLICABILITY:

Regulation XI-2/6 applies to the following types of vessels on international voyages:

(a) Passenger ships, including high-speed passenger craft;
(b) Cargo ships, including high-speed craft, of 500 gross tons and upwards; and
(c) Mechanically propelled mobile offshore drilling units as defined in regulation IX/1, not on location.

REQUIREMENTS:

1.0 <u>Implementation</u>

1.1 All ships in the above general categories shall be provided with an SSAS as follows:

.1 Ships constructed on or 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 after 1 July 2004;

.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 radio installation after 1 July 2004; and

.4 Other cargo ships of 500 gross tonnage and upwards and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of radio installation after 1 July 2006.

1.2 Regarding compliance with the additional functional requirements of MSC/Circ.1190, ships in the above general categories shall be provided with a compliant or upgraded SSAS as follows:

.1 Ships constructed on or after 1 July 2006, compliant;

.2 Passenger ships, including high-speed passenger craft, constructed before 1 July 2006, not later than the first survey of the radio installation after 1 July 2006, upgrade;

.3 Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before 1 July 2006, not later than the first survey of radio installation after 1 July 2006, upgrade; and

.4 Other cargo ships of 500 gross tonnage and upwards and mobile offshore drilling units constructed before 1 July 2006, not later than the first survey of radio installation after 1 July 2006, upgrade.

1.3 All Ship Security Alerts (SSAs) generated by an SSAS shall be sent to the RMI Maritime Administrator (the "Administrator") and Company Security Officer (CSO).

1.4 SOLAS Chapter XI-2, Regulation 6, requires all ships to be provided with an SSAS, which will transmit a security alert to a designated, competent authority when activated in an emergency situation. As the ship security alert system is a requirement of SOLAS Chapter XI-2, it is not considered to be radio equipment, thus not covered by the Safety Radio Survey, and the Safety Radio certificate is not affected. Any deficiency in the ship security alert system, however, is a failure in compliance with the ISPS Code and potentially the ISM Code.

2.0 Competent Authority

2.1 A competent authority is an organization that receives an alert from a vessel and forwards it to the Administrator and the CSO. A competent authority must demonstrate the capability to receive an SSA at any time from a vessel and to immediately forward it.

2.2 Providers of asset tracking services, such as Globe Wireless, PurpleFinder, Transas, Iridium, etc., incorporating SSAS capabilities, may act as the competent authority.

2.3 Companies or organizations desiring to provide SSAS services for RMI flagged vessels should provide the Administrator with a detailed description of the equipment to be installed or modified and a coordinated communications plan for acting as a competent authority. The details of this system: equipment, coverage area, and communications plan, should also be submitted to the RSO for review.

2.4 Companies desiring to send SSAs directly to the Administrator and CSO or organizations desiring to act as competent authorities for the forwarding of SSAs to the Administrator and CSO should confirm the technical arrangements for delivering SSAs to the Administrator with the Radio Services Area Administrator at the following address:

Marshall Islands Maritime and Corporate Administrators
11495 Commerce Park Drive
Reston, Virginia 20191-1506 USA
Tel: +1-703-620-4880
Fax: +1-703-476-8522
Email: nsantram@register-iri.com

2.5 An SSA email address and phone number will be provided to the CSO by the Administrator on request during the installation process.

3.0 Ship Security Plans

3.1 SOLAS vessels are required to have SSASs documented in their security plans. The Administrator's RSO will review a vessel's SSAS equipment and procedures in conjunction with their review of the vessel's security plan. The location of the second activation point may be specified in the Ship Security Plan and remain confidential. However, in order to avoid the possibility of compromising the objective of the ship alert system, the Administrator is recommending that this information be kept elsewhere on board in a document known only to the Master, Ship Security Officer and other senior ship's personnel as may be decided by the CSO.

3.2 If a vessel already has an approved security plan, the plan must be amended to address the SSAS, and affected parts must be available on board for review and approval during the compliance audit following initial installation. This should include documentation of any equipment that may be installed to comply with these regulations for that particular vessel.

3.3 Necessarily, the continued validity of a vessel's initial International Ship Security Certificate will rely upon, among other things, compliance with the installation of an effective SSAS by the applicable Safety Radio Survey implementation date irrespective of when the ship security system may be due for intermediate or renewal audit.

3.4 Systems installed on vessels not required to carry SSAS equipment should generally meet these requirements.

4.0 System Requirements

4.1 Performance standards for SSASs are given in IMO Resolution MSC.136(76) as amended by MSC.147(77). MSC/Circ.1072 and MSC/Circ.1155 give further guidance on the design and functional requirements of SSASs provided to comply with the SOLAS regulation.

4.2 The SSAS may be a component of existing radio installations, but it may not interfere with the normal function of that equipment. If the SSAS uses any new or modifies existing radio transmission equipment, then the supplier must certify the equipment. Any new electronic equipment must be certified by the manufacturer to comply with the relevant sections of IEC 60945 that are identified as being required for all equipment categories.

4.3 If the SSAS uses the ship's main source of electrical power, a suitable backup service should be provided. This may be an existing alternate source or dedicated battery backup. For these systems an uninterruptible power supply (UPS) or similar device, powered from the ship's main power is considered to be an alternate source of power.

5.0 Application

5.1 The transmission of a security alert should not be included with any other routine reporting that the ship may conduct. The message transmission should be generated automatically with no input from the operator other than the activation of the system. Cellular telephones may not be sufficiently automated to satisfy this requirement. To comply with MSC/Circ.1190 and RMI requirements, the message eventually received by a competent authority must include:

(a) the vessel name;
(b) the IMO Ship Identification Number;
(c) the Call Sign;
(d) the Maritime Mobile Service Identity
(e) date and time;
(f) position;
(g) course and speed;
(h) name of CSO and 24/7 phone number;
(i) name of alternate CSO and 24/7 phone number; and
(j) a message stating that the SSAS has been activated and indicating the ship is under threat or it has been compromised,

5.2 If using asset tracking services, an active hyperlink to the monitoring agency is to be provided in the message. The hyperlink should operate either automatically or be accessible to the Administrator by use of a unique user I.D. and password assigned to the Administrator. This information will expedite the Administrator's ability to contact the nearest Coastal State Designated Authority and the CSO when a security alert message is received.

5.3 The security alert transmission must be capable of reaching the Administrator and CSO from any point along the vessel's intended route. This alert should not be transmitted as a general distress call. It should be directed solely to the Administrator and CSO. As previously authorized, this may be accomplished through a competent authority.

5.4 Line-of-sight transmissions such as encrypted radio transmissions will be closely evaluated, and depending on the route of the vessel may be accepted.

6.0 Initial Installation and Type Approval

6.1 Vessel owners are required to notify the RSO prior to installing an SSAS.

6.2 Due to their mode of installation and operation, there are effectively two (2) types of ship security alert systems commonly known as Ship Security Alert Systems (SSAS) and Self-Contained SSAS (SSAS-SC). Companies should be aware of the difference and which type they have fitted to their ships so that the appropriate software and interfaces are provided to assure the ultimate receipt of all required information listed in section 5.1 above by the competent authority.

6.3 The Administrator will not complete any formal type approval for SSASs or SSAS-SCs. Vessel specific systems will be reviewed and approved by the Administrator's RSO during the vessel's security plan review. A list of RSOs with their contact information is available from the Administrator's website www.register-iri.com under Marine Safety Advisories.

7.0 "SSAS

7.1 This is a system which requires interface with, and/or depends on input from, radio and/or navigational equipment required by SOLAS IV and V to meet the performance standards required by SOLAS Regulation XI-2/6. The SSAS is a requirement of SOLAS Chapter XI-2 and is not subject to Safety Radio Certification.

7.2 In all cases, the RO responsible for the issue of the Safety Radio Certification shall be responsible for the initial installation inspection and testing of the SSAS by an approved radio technician.. A copy of the radio technician's report, demonstrating compliance with SOLAS XI-2/6 Paragraphs 2-4 inclusive and MSC/Circ.1190, shall be left on board for use by the RSO at the next scheduled audit. A comment such as "The SSAS as fitted meets the requirements of SOLAS Regulation XI-2/6, paragraphs 2-4 inclusive and MSC/Circ.1190." shall be entered into the Record of Approved GMDSS Radio Installation. It should be noted that the record of equipment for the Cargo-Ship Safety Radio Certificate Form "R" shall not include details of the SSAS. The SSAS installation shall be subject to annual inspection by an approved radio technician.

8.0 SSAS-SC

8.1 This is a system which does not require any interface with, and/or depends on input from, radio and/or navigational equipment required by SOLAS IV and V to meet the performance standards required by SOLAS XI-2/6. However, software revisions may be necessary on

existing installations to bring the system in compliance with the added information required by MSC/Circ.1190. This equipment is installed and initiated by the ship and no initial installation survey is required. An SSAS-SC may be tested and reported by the SSO.

9.0 Shipboard Verification

9.1 At the next ISPS ship board verification following the initial installation of the SSAS or SSAS-SC, the auditor shall review and approve the related provisions in the SSP, witness a complete security alert test and verify the implementation of the operational requirements of the SSAS or SSAS-SC in accordance with the requirements of ISPS Code A/9.4.17 to A/9.4.18 and, in the case of an SSAS, sight the Record of Approved GMDSS Radio Installation, the Statement of Compliance or equivalent.

9.2 At each subsequent ISPS verification the auditor shall examine the records of activities on the SSAS or SSAS-SC specified in ISPS Code A/10.1.10, witness a complete security alert test and verify the operational requirements and in the case of an SSAS, sight the Record of Approved GMDSS Radio Installation, the Statement of Compliance or equivalent.

9.3 A "complete" security alert test shall require the sending of a test message to the CSO and the Administrator.

10.0 Testing

10.1 Following the initial installation of the SSAS or SSAS-SC, the Company has the responsibility:

- to ensure that the system is tested and maintained to satisfy operational requirements according to the approved SSP; and
- to keep on board the system records specified in ISPS Code A/10.1.10.

10.2 The system shall be capable of being tested to verify proper operation. The testing should include the entire alert system, from activation to CSO receipt of the alert.

10.3 The unit should also be capable of being tested in the presence of a port State control inspector upon request, but only from the required navigation bridge location and with appropriate prior notification of the CSO and the Administrator.

10.4 The procedures for this testing, including the appropriate Administrator phone numbers and security email address, should be outlined in the vessel's security plan or in a separate document available only to the Master, SSO or other entrusted senior ship's officer.

10.5 The Administrator should be notified in advance of any test that will result in a message being sent to the Administrator. Arrangements should also be made in advance with the Administrator for those tests requiring the Administrator to verify receipt.

10.6 CSOs are reminded that the Administrator should only be receiving test alerts on the following occasions:

- Installation of the SSAS or SSAS-SC system;
- Intermediate Audit/Survey for ISSC Certification; and
- Renewal Audit/Survey for ISSC Certification.

10.7 The test message should be marked "TEST."

10.8 Testing shall be properly logged in the Official Log.

11.0 Activation

11.1 The activation of a security alert should only require a single action, excluding the opening of protective covers. There must be at least two (2) activation points. One (1) must be located on the navigation bridge and at least one (1) other in an area where it would normally be immediately accessible, e.g., engine room control, master's stateroom, crew lounge, etc. The activation points must not be capable of deactivating the alarm once initiated and must be protected against inadvertent operation. The activation point should not be protected by seals, lids or covers that must be broken to activate the alarm since a broken seal would indicate that the alarm has been tripped. Spring loaded covers or similar devices that provide no indication of the status of the alarm are acceptable.

11.2 Once activated, the system should continue to transmit the security alert at a frequency of not less than once per 30 minutes until the status of the alert is confirmed by the CSO and authorization is given by the CSO for the alarm to be reset or deactivated. There should be a confidential procedure to properly verify the status of the alert and any resetting or deactivation of the system. The vessel should initiate the deactivation of the system, unless it can be done remotely by the CSO.

11.3 When the Administrator receives an SSA the status of which cannot be readily confirmed, the Administrator will immediately notify the Coastal State(s) in the vicinity of which the ship is presently operating. It is therefore imperative that the CSO verify immediately the status of each SSA with the Administrator and that false alarms be avoided.

12.0 Ship Security Report System (SSRS)

Shipowners are authorized and strongly recommended to subscribe to the SSRS because it provides a real-time link between ship operations and naval operations thereby enhancing the counter-piracy effectiveness of the existing SSAS. Refer to MN 2-011-31 for details.