CCS 通 函
Circular

China Classification Society
(2012) Circ. No. 55 Total No.217
May 29, 2012 (Total 14 Pages)

TO: Related departments of CCS Headquarters; Branches and Offices; and Ship Companies

SHIP SECURITY ALERT SYSTEM (SSAS)

--Marshall Marine Notice No.2-011-18, Rev. 2/12

The Office of The Maritime Administrator of Marshall Island issued the Marine Notice No.2-011-18, Rev. 2/12 to explain the functional and national requirements of the SSAS as it applies to the Republic of the Marshall Islands (RMI) flagged vessels. It also 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. The 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. All the auditors of CCS branches and offices should comply with the requirements of this notice during relevant inspections and audits.

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 Implementation

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 SelfContained 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.

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.