U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-3PCV
Phone: (202) 372-1251
Fax: (202) 372-1917
Email: fldr-g-pcv@comdt.uscg.mil

COMDTPUB 16000.4
NVIC 04-03, CH-2

DEC 15 2006

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 2

Subj: CH-2 to GUIDANCE FOR VERIFICATION OF VESSEL SECURITY PLANS ON DOMESTIC VESSELS IN ACCORDANCE WITH THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS AND INTERNATIONAL SHIP & PORT FACILITY SECURITY (ISPS) CODE

Ref: (a) International Convention for the Safety of Life at Sea (SOLAS), Chapter XI-2/6
(b) International Ship & Port Facility Security (ISPS) Code
(c) International Maritime Organization MSC Circulars 622, 623, 1073, and 1190
(d) Title 33 Code of Federal Regulation, Part 101
(e) Title 33 Code of Federal Regulation, Part 104
(f) Maritime Law Enforcement Manual, COMDTINST M16247.1C

1. PURPOSE. This change to NVIC 04-03 provides additional guidance regarding Ship Security Alert Systems (SSAS) and vessel audit procedures. Specifically, additional guidance is provided regarding the format of ship security alert messages, the United States' response to receiving these messages, as well as recommended procedures to verify an alert message.

2. ACTION.

a. Coast Guard Captains of the Port (COTP) and Officers in Charge, Marine Inspection (OCMI) are encouraged to bring this circular to the attention of marine interests within their zones of responsibility. This circular will be distributed by electronic means only. It is available on the World Wide Web at http://www.uscg.mil/hq/g-m/index.htm.

DISTRIBUTION – SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		8	*		5									150	1	1	2									5
C					*								*													
D	1	2		1*	1						1*	*														
E														2	*											
F			1							1																
G																										
H																										

NON-STANDARD DISTRIBUTION: See Page 3

b. These guidelines may be applied to evaluate, or document vessel SSASs and vessel security audits.

3. DIRECTIVES AFFECTED. Remove NVIC 04-03 Change 1, Enclosure 5, and insert NVIC 04-03, Change 2, Enclosure 5. Also insert NVIC 04-03, Change 2 Enclosure 9.

4. BACKGROUND. The attached enclosures provide guidance on implementing the International Convention for the Safety of Life at Sea (SOLAS), Regulation XI-2/6 as it applies to U.S.-flag vessels. It is intended to provide information for U.S. Coast Guard field offices, vessel owners and operators, and others involved with ship security alerting. This change to the NVIC provides guidelines for developing systems to meet the requirements of SOLAS, Regulation XI-2/6, as well as 33 CFR 104.415.

5. DISCUSSION. This revised circular provides guidance to COTPs and OCMIs on the requirements for SSAS and how to evaluate the systems for compliance with references (c), (d), and (e). For the purpose of this guidance, the term "area" is defined as a COTP zone. The revised circular also provides audit guidance to COTPs and OCMIs.

6. INFORMATION SECURITY.

a. Information regarding the submission and response to SSAS and vessel auditing procedures are part of the Vessel Security Plan (VSP), which contains information that, if released to the general public, could compromise the safety or security of the vessel, the port and its users. This information is known as Sensitive Security Information (SSI), and the Transportation Security Administration (TSA) governs SSI through 49 CFR 1520, titled "Protection of Sensitive Security Information." These regulations allow the Coast Guard to maintain national security by sharing unclassified information with various vessel and facility personnel without releasing SSI to the public. Vessel and facility owners, Area Maritime Security Committees (AMSCs), and waterway operators must follow procedures stated in 49 CFR 1520 for the marking, storing, distributing and destroying of SSI material which includes many documents that discuss screening processes and detection procedures.

b. Under these regulations, only persons with a "need to know," as defined in 49 CFR 1520.5, will have access to information regarding SSAS. Vessel owners or operators must determine which of their employees need to know provisions of the security plans and information about the SSAS, and then restrict dissemination of these documents accordingly. To ensure that access is restricted to only authorized personnel, SSI material will not normally be disclosed under the Freedom of Information Act (FOIA).

c. When SSI is released to unauthorized persons, a report must be filed with the Department of Homeland Security. Such unauthorized release is grounds for a civil penalty and other enforcement or corrective action.

7. DISCLAIMER. While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it itself a rule. Thus, it is not intended to, nor does it, impose legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.

8. FORMS/REPORTS. None.

C. E. BONE
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Operations

Encl: (1) Ch-2 to Navigation and Inspection Circular 04-03 enclosure 5 Ship Security Alert Systems
(2) Ch-2 to Navigation and Inspection Circular 04-03 enclosure 9 Vessel Auditing Guidelines

Non-Standard Distribution:
DOJ Torts Branch (Washington, DC; New York; San Francisco only) (1)
MARAD (MRG 4700) (1)
MSC (M-24) (1)
NOAA Fleet Inspector (1)
NTSB (Marine Accident Division) (1)
World Maritime University (1)
U.S. Merchant Marine Academy, Kings Point, NY (1)
State University of New York Maritime College (1)
California Maritime Academy (1)
Maine Maritime Academy (1)
Massachusetts Maritime Academy (1)

ENCLOSURE 5

SHIP SECURITY ALERT SYSTEMS

ENCLOSURE 5
SHIP SECURITY ALERT SYSTEMS

1. Introduction:

   A. This enclosure provides guidance on implementing the International Convention for the Safety of Life at Sea (SOLAS), Regulation XI-2/6 as it applies to U.S.-flag vessels. It is intended to provide information for U.S. Coast Guard field offices, vessel owners and operators, and others involved with ship security alerting, as well as provide guidelines for developing systems to meet the requirements of SOLAS, Regulation XI-2/6.

   B. U.S. Coast Guard marine inspectors should review the guidance contained in this section to determine if a ship security alert system (SSAS) installed on an U.S.-flag vessel is suitable for its intended purpose, and that it is in compliance with the requirements of SOLAS, Regulation XI-2/6.

   C. SSAS has been developed to provide a vessel master or operator the ability to send a covert alert to shore regarding a security threat to the vessel. SOLAS, Regulation XI-2/6, which requires the fitting of SSASs on certain SOLAS certified vessels, was adopted in December 2002 in conjunction with the International Ship and Port Facility Security (ISPS) Code. Performance standards for the SSAS were adopted by the International Maritime Organization (IMO) in MSC Resolution MSC.147 (77). This document is available at the following address: http://www.navcen.uscg.gov/marcomms/imo/msc_resolutions/default.htm.

   D. SSAS alerts originate aboard the threatened ship, and are transmitted by communications service providers (that provide mobile satellite, terrestrial radio, or ground links) to competent authorities designated by the vessel's flag state, and are relayed to the flag state. The flag state is then responsible for notifying appropriate authorities of coastal states in the vicinity of the ship or other states as appropriate.

   E. SSASs are one-way, ship-to-shore alerting systems for situations where lives may be in grave and imminent danger. Therefore, it is essential that the SSAS on board vessels, satellite links, land earth stations, ground communications, and other elements used in transmitting or relaying security alerts to competent authorities ashore be fast, function properly, and be highly available and reliable. These alerts are not "distress alerts" covered by separate requirements of IMO and the International Telecommunications Union, but are comparable and intended to address equally dangerous shipboard situations. Since the SSAS is comparable to equipment used to provide distress alerts to search and rescue authorities, the SSAS and its associated satellite and shore systems should meet comparable standards.

   F. Ships have various communications channels or methods available to help deal with acts of violence that pose security threats to ships, and are used for alerting, assisting with the response, resolving inadvertent alerts, and submitting follow up reports. In the event of an

actual, developing, or apparent security threat, or when the security of the ship has actually been compromised, SSASs are not the only allowable means of alerting the Administration or Competent Authority of security threats to vessels. If suspected attacks are detected early, or if suitable opportunities arise that would not further endanger persons onboard, other means of communications may be used.

2. Definitions: The following terms and definitions relate to security threats and alerting terminology:

Activation: The human intervention aboard the ship that sets in motion the automated alert system.

Acts of Violence: Acts of terrorism and violent acts that threaten the vessel's security, piracy, acts of armed robbery against ships, and any other security incidents directed against a ship, where the term "ship" is understood to include all persons on board.

Communications Service Provider (CSP): An entity responsible for all or part of the delivery of security alert messages from ships to recognized Administrations, competent authorities, or Tracking Service Providers (TSP).

Competent Authority: Designated authority that receives SSAS alerts from ships and informs the appropriate Administration. See Paragraph 5 of this document for guidance regarding competent authorities.

Priority Access: Treatment given by communications systems to place distress and ship security alerts and calls ahead of all other traffic.

Satellite System: The space segment, land earth station (or equivalent), and arrangements for controlling the space segment and the network control facilities governing access.

Ship Security Alert System (SSAS): Shipboard system required by SOLAS Regulation XI-2/6 to covertly send an alert to a competent authority of a vessel's flag state indicating a security threat to the vessel.

Test Mode: Resetting, delaying or preventing the transmission of an alert for the purposes of testing during inspections.

Tracking Service Provider (TSP): An entity that is responsible for all or part of the delivery of security alert messages from either ships or CSPs to competent authorities.

Transmission Termination: The human intervention aboard the ship that legitimately stops the automated alert system. This could include keying in a combination or password or pushing a button. Termination can't be done from the activation device and does not cancel the alert.

3. Compliance Dates: The following SOLAS vessels are required to install SSAS equipment:

   A. Ships constructed on or after 1 July 2004;

   B. Passenger ships, including high-speed passenger crafts, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;

   C. Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed crafts, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004; and

   D. Other cargo ships of 500 gross tonnage and upward, and Mobile Offshore Drilling Units (MODUs) constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.

4. Voluntary Compliance: SSASs may also be voluntarily installed aboard other vessels. Such installations should generally comply with the requirements of this Circular, particularly with regard to SSAS approval, registration, and testing.

5. Competent Authority:

   A. SOLAS XI-2/6 allows the Administration to designate a competent authority to receive alert signals from vessels. The Coast Guard, acting as the Flag Administration, has chosen to retain the responsibility of receiving alert messages. Specifically, Rescue Coordination Center (RCC) Alameda, a Coast Guard unit equipped to handle such duties, is the only U.S. entity authorized to receive such alerts. RCC Alameda will work closely with Headquarters and Operational Commanders to relay all alert information. This information will be used to coordinate response protocol for vessels operating within U.S. waters and those operating abroad. No other competent authorities will be designated by the United States for the purposes of receiving SSAS alerts.

   B. Contact information for RCC Alameda is as follows:

Address:	Commander, U.S. Coast Guard Attn: RCC Alameda Coast Guard Island Alameda, CA 94501
Voice:	(510) 437-3701
Fax:	(510) 437-3017
Telex:	230172343
E-mail:	ssas@uscg.mil

C. Voice reports of an alert are preferred. While email and fax reports are acceptable under international protocol, it is recommended that such reports are followed up by a phone call. The follow-up phone call is critical, as it provides RCC Alameda an immediate point of contact to assist in the validation of the ship security alert.

D. It should be noted that the National Response Center (NRC), a clearinghouse for most maritime emergency notifications, should NOT be contacted for a ship security alert, and is not set up to receive reports of a ship security alert.

E. RCC Alameda, as the recipient of the SSAS alerts, will also be the primary agency documenting the reports in accordance with the Marine Information for Safety and Law Enforcement (MISLE) SSAS Alert Documentation Guide available at: http://mislenet.osc.uscg.mil/.

6. Submission of System Details for Approval:

A. The U.S. Coast Guard will not complete a formal type approval for SSASs. Each SSAS will be evaluated for compliance with the performance standards in MSC.147 (77), the technical requirements of this NVIC and, as applicable, as part of the Security Plan approved for the vessel. Companies or organizations desiring to provide SSAS services for U.S. vessels may provide the U.S. Coast Guard with a detailed description of the equipment to be installed or modified. Companies or organizations wishing to act as Communications Service Providers (CSPs) may provide details of their capabilities to monitor and forward alerts to the U.S. Coast Guard. This information should be submitted to Commandant (CG-3PSE-3) for review at the following address:

Address: Commandant (CG-3PSE-3)
2100 Second Street, SW
Washington, DC 20593-0001
Voice: (202) 372-1378
Fax: (202) 372-1925

B. Vessel specific details of each SSAS will be reviewed and approved by the U.S. Coast Guard Marine Safety Center (MSC). For security purposes, the details and procedures for an SSAS installed on board a vessel should be contained in a separate annex or supplement to the vessel's security plan and stored separately from the plan to limit access to its details. Access to this annex should be limited to the master, vessel security officer, and other senior personnel designated by the shipping company. The SSAS information does not need to be submitted to the MSC until required according to the implementation schedule. The majority of U.S.-flag SOLAS vessels will likely submit their SSAS information to MSC after the U.S. Coast Guard has already approved their security plan. If a vessel has a previously approved plan, only the annex covering the SSAS needs to be submitted for review. MSC's address for visitors and courier service is the following:

Address:	Commanding Officer (MSC) USCG Marine Safety Safety Center Jemal Riverside Building 1900 Half Street SW, Suite 1000, RM 525 Washington, DC 20024
Voice:	(202) 475-3444
Fax:	(202) 475-3920

7. Installation of SSAS on board SOLAS Vessels: U.S. Coast Guard Officers in Charge, Marine Inspection (OCMIs) will verify the correct operation of all SSASs installed on board U.S. vessels subject to SOLAS Regulation XI-2/6, and verify the SSAS installation complies with the system described in the approved Vessel Security Plan.

8. System Requirements:

   A. SSASs should comply with the provisions of MSC.147 (77) on performance standards for ship security alert systems. The transmission of a security alert should not be included with any other routine reporting that the ship may conduct. The activation of a security alert should only require a single action to exclude the opening of protective covers. There must be at least two activation points: one must be located on the navigation bridge and at least one 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 it has been initiated and it must be protected against inadvertent operation. Seals, lids or covers that must be broken, or buttons that remain depressed upon activation of the alarm, may not be used since a broken seal or depressed button would indicate that the alarm has been tripped. Spring loaded buttons, covers, or similar devices that provide no indication of the status of the alarm are acceptable. Activation of the SSAS should not cause any alarm or indication to be raised on the ship or near the activation point.

   B. If the SSAS uses the ship's main source of electrical power, a suitable backup service should be provided to sufficiently and properly power the SSAS for at least 24 hours. This backup service 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 may be used for an alternate source of power.

   C. 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 radio transmission equipment or modifies existing radio transmission equipment (except for software modifications that do not affect transmission characteristics), then the Federal Communications Commission (FCC) must certify the equipment. Any new electronic

equipment must be certified by the manufacturer to comply with the relevant sections of IEC 60945 [1] that are identified as being required for all equipment categories.

D. The relevant CSP should certify specific SSAS equipment as acceptable if the alerts are processed via a maritime mobile satellite system.

E. SSASs should generally meet the requirements and standards applicable to other distress alerting equipment as follows:

1. SSASs that operate through the Cospas-Sarsat system should generally meet the relevant requirements for Electronic Position Indicating Radio Beacons (EPIRBs) contained in 47 CFR 80.1061, 1101, and 1103, and should be registered and labeled similar to the requirements for EPIRBs contained in 47 CFR 80.1061. These regulations establish requirements for radio emissions, test facility certification, submission of information to the Coast Guard and FCC, coding, labeling, and registration.

2. SSASs that operate through the Inmarsat system should generally meet the relevant requirements for Inmarsat ship earth stations contained in 47 CFR 80.1101 and 1103. These regulations establish requirements for radio emissions, type approval by Inmarsat, and submission of information to the FCC for certification. Inmarsat SSASs should be registered with Inmarsat in accordance with IMO Assembly Resolution A.887 (21).

3. SSASs that rely on encrypted terrestrial radio transmissions should be closely evaluated, and may be acceptable depending on the route of the vessel; however, if this approach were employed, encryption provisions satisfactory to the Coast Guard would have to be used with arrangements for maintenance of the encryption key.

4. Other equipment proposed for use as SSASs on U.S.-flag vessels should also be certificated by the FCC and accepted by the Coast Guard for its intended use. How the equipment complies with the recognized national or international standards should be noted in the manufacturer's documentation provided with the equipment. Generally, such equipment should meet performance and registration requirements comparable to those cited for equipment operating through Cospas-Sarsat and Inmarsat as discussed above if maritime mobile satellite systems are used, or comparable to the relevant provisions of 47 CFR Part 80 for terrestrial systems. For vessels away from coastal areas, cellular phones and electronic mail are not generally considered suitable means of delivering ship security alerts to competent authorities due to typical limits on reliability and automatic processing.

---

[1] International Electrotechnical Commission (IEC) Publication IEC 60945 (2002) "Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results"

5. Radio equipment used for SSASs may operate on appropriate emergency frequencies designated for distress communications.

9. Equipment Registration: Equipment should be appropriately registered to ensure that 24/7 arrangements are in place for retrieval of SSAS information by competent authorities. The registration data may be maintained by the CSP or other suitable entity and ideally should be retrieved automatically and forwarded with a ship security alert. The ship owners or operators are responsible for ensuring that this data is up-to-date.

10. Ship Security Alert Messages:

A. Alert messages should be generated automatically with no input from the operator other than the activation of the system, and must be capable of reaching the competent authority from any point along the vessel's intended route. This alert should not be transmitted as a general distress alert. Once activated, the SSAS should continue to transmit the security alert until the equipment is reset or deactivated. The interval between transmissions of the alerts should ideally be between 15 minutes and one hour. Ship security alert messages should only be sent to the shore stations that are outlined in the vessel security plan's SSAS annex. Ship security alert messages should not be sent to ship stations.

B. The format of ship security alerts should be compatible with the communication system used to transmit it and, as a minimum, contain the following:

1. Ship's identity (e.g., IMO number, Inmarsat IDs (including ocean regions code), Maritime Mobile Service Identity (MMSI) number, or call sign);

2. Ship's position (latitude and longitude associated with a date and time); and

3. Ship's security alert activation indication.

C. Messages should be transmitted at distress priority (or priority 3 if the system transmits via Inmarsat).

D. Alert messages are difficult to validate because international regulations prevent direct contact with the vessel in question. However, investigation into the alert using sources on board the vessel is feasible if conducted properly. The IMO Maritime Safety Circular 1072, of 26 June 2003, allows a system that utilizes the exchange of messages containing key words between a ship and the ship's company via speech or data communications. In no instance will the U.S. Coast Guard directly contact the vessel during the initial investigation of an alert. Other actions that might help to validate an alert are:

1. When predetermined check-in times are established, and a vessel misses a check-in which is immediately followed by an alert;

2. If a security alert is received in conjunction with a distress alert;

3. If a partial, obscure, or incomplete transmission precedes a security alert; or

4. If a predetermined "codeword" is received (keywords and/or phrases that under normal circumstances would be standard but may have alternate answers that would indicate a problem).

E. Whatever mechanism is employed, its existence and format should be available only to a select number of persons on board the vessel and the entity (e.g. Ship's Company, TSP, or CSP) responsible for forwarding the alert to RCC Alameda. Additionally, these validation methods should not be used if they could endanger the crew or ship, or raise suspicion. The mechanism should be changed frequently, especially the use of a "codeword," and proper training should be conducted on a regular basis. Whatever mechanism is used to validate an alert, the details should be described in the SSAS Annex to the VSP. RCC Alameda should also be advised of the validation mechanism upon the initial investigation of a ship security alert.

11. Termination and Post Incident Reports:

A. RCC Alameda is to be notified by the appropriate entity, such as the Company Security Officer (CSO), the vessel owner or owner's agent, or the competent authority (for foreign vessels) when an alerted security threat has ended. Additionally, it is important to report all threats to vessel security in which the ship's SSAS has been activated, whether successful or unsuccessful, to RCC Alameda. This information is used to reduce the risks of future incidents, improve preparedness to respond to such incidents, and enable the U.S. Government to comply with mandatory reporting requirements to the IMO.

B. This post-incident report should be submitted in the following format:

1. Ship's name and call sign, IMO number, Inmarsat ID, or MMSI number;

2. Reference initial ship security alert;

3. Name of the area
Position of incident (Latitude and longitude)
Time of incident;

4. Details of incident, e.g.,
   - While sailing, at anchor or at berth?
   - Method of attack
   - Description/number of suspect craft
   - Number and brief description of attackers/perpetrators
   - What kind of weapons did the attackers carry?

- Any other information (e.g., language spoken)
- Injuries to crew and passengers
- Damage to ship (Which part of the ship was attacked?)
- Brief details of stolen property/cargo
- Actions taken by the master and crew
- Was incident reported to the coastal authority and to whom?
- Action taken by the coastal state;

5. Last observed movements of pirate/suspect craft (e.g. Date/time/course/position/speed);

6. Assistance required;

7. Preferred communications with reporting ship, e.g.,
   Appropriate Coast Radio Station
   HF/MF/VHF
   INMARSAT IDs (including ocean region code)
   MMSI; and

8. Date/time of report (UTC).

12. Inadvertent or False Ship Security Alerts:

A. The ship should report an inadvertent alert to RCC Alameda immediately to protect system integrity and to prevent a costly response that may divert response resources from a bona fide emergency.

B. False alerts are extremely costly, occupying time and resources that become unavailable to respond to valid events. The Coast Guard intends to prosecute vessels or people making false alerts if it is determined that the false alerts are intentional. The nature of an alert and the response multiplies the effect of a false alert.

13. Communications Service Providers:

A. A CSP receives radio security alerts from ships and relays them to either competent authorities, TSPs, or Flag Administrations using capabilities such as satellite systems, terrestrial radio systems, and ground communications links.

B. Global Maritime Distress and Safety System (GMDSS)-based CSPs already operating as an IMO-recognized part of GMDSS need not undergo further approval to process ship security alerts as long as these alerts are handled in a manner equivalent to GMDSS distress alerts, and are routed to U.S. designated competent authorities.

C. Non-GMDSS-based CSPs using mobile satellite systems not yet or not intending to be recognized by IMO as part of GMDSS will need to be reviewed by the U. S. Coast Guard

Office of Systems Engineering (CG-3PSE-3) for suitability with the applicable provisions of IMO Assembly Resolution A.888 (21). Non GMDSS-based CSPs will also need to be reviewed by the Federal Communications Commission (FCC). Non-GMDSS CSPs are to be capable of doing the following:

1. Provide continuous coverage in areas where ships using the system will sail with at least 99.9% network availability;

2. Be able to handle the anticipated distress priority traffic by vessels using the system;

3. Automatically route ship security alerts to the appropriate designated competent authorities or TSPs;

4. If practicable, advise vessels, competent authorities, and TSPs of any outages or scheduled downtime before or when they occur; and

5. Continuously monitor and record network availability and provide a report on the recorded availability to the Commandant (CG-3PSE-3) at least once every year.

D. Store and forward systems should have arrangements in place to ensure that ship security alerts are promptly delivered.

E. CSPs should make every effort to be able to provide current vessel critical data to RCC Alameda. The data should be maintained by the CSP or another suitable entity and, ideally, should be retrieved automatically and forwarded with a ship security alert. The data should include vessel information/identification and 24 hour contact information for a responsible person that may assist RCC Alameda in validating a ship security alert. If the data is maintained on a password protected website, arrangements will need to be made to provide RCC Alameda a login name and password to facilitate response efforts to an alert.

F. A CSP should be able to demonstrate that they can reliably perform these functions without actually processing an alert through to the competent authority, i.e., it should be able to show upon request from a U.S. Coast Guard authority that it can automatically relay a message at the appropriate distress priority through its system up to the point where it is handed off to the next CSP or TSP in the system to the competent authority.

G. Once a CSP is supporting the transmission and relay of ship security alerts for vessels, a two year written notice should be given to the U.S. Coast Guard and relevant vessel owners for the withdrawal of such services, unless vessels are no longer using the service or unless otherwise approved by the U.S. Coast Guard.

13. Tracking Service Providers (TSP's):

A. A TSP monitors the transmission reports and receives the radio security alerts via the

CSP and informs competent authorities and the CSO when the transmission format changes.

B. In such cases where the SSAS alert is sent only to the TSP and is not automatically routed to the competent authority, the TSP must show that it is in accordance with the applicable provisions of IMO Assembly Resolution A.888(21) and their ability to meet the guidelines in this section. The TSP's compliance statement must be submitted with the vessel's security SAS annex.

C. In lieu of submitting all of the documentation to demonstrate compliance with the entire section 13A(1), TSPs already accepted/approved to receive GMDSS alerts are only required to submit documentation showing their GMDSS acceptance/approval. (TSPs accepted/approved to receive GMDSS alerts are already verified by the International Mobile Satellite Organization (IMSO)).

D. TSPs should:

1. Operate a dedicated watch in continuous operation 24 hours a day, seven days a week for 365 days a year;

2. Be able to connect to RCC Alameda;

3. Keep continuous watch on appropriate satellite communication channels; and

4. Be capable of processing the information received with the highest priority.

E. Priority:

1. The TSP should be capable of automatically recognizing the priority of ship-to-shore communications and should preserve the priority and process maritime mobile communications for the following four levels of priority:
   a. Distress;
   b. Urgency;
   c. Safety; and
   d. Other communications.

2. Priority access should be given for distress alerts and calls in real time.

3. The TSP must have reliable communication links to RCC Alameda.

4. The communication links for mobile-satellite voice communication systems, or data communications systems, should be connectable to the public switched network in accordance with relevant International Telecommunication Union (ITU) recommendations.

F. U.S. Flagged vessels may be required during inspection and testing of their SSAS to provide adequate documentation proving that the CSP/TSP with which they have contracted, meets the requirements as above. The documentation will be kept by the vessel as part of it's VSP with the details of system operation.

G. Should a TSP that is supporting the transmission and relay of ship security alerts for vessels have to withdraw its services, the TSP must notify the U.S. Coast Guard and relevant owners of the withdrawal and allow sufficient time for the affected vessel(s) to obtain services from another CSP or TSP.

14. SSAS Inspection and Testing:

A. The SSAS should be capable of being tested, upon request by a marine inspector, without inadvertently sending a live transmission. Procedures for testing should be outlined in the vessel's security plan. SSAS testing shall be logged in accordance with 33 CFR 104.235. Marine inspectors are not to send a live transmission to RCC Alameda when inspecting SSAS units aboard vessels.

B. Testing procedures for SSAS systems are indicated by the type of SSAS system employed aboard the vessel. Coast Guard Inspectors or other approving officials must consult system documentation to determine if the unit is installed and functioning properly. The results of a successful test may be a message received at the vessel's CSP/TSP, an indicator light upon the unit itself, or the reception of routine fleet management data from the unit. In general, the testing procedures should be carried out according to the following (or equivalent) procedures, as appropriate for the particular SSAS:

1. Carry out a self-test routine for internal circuitry and emissions, in accordance with the SSAS manufacturer's instructions or handbook;

2. Confirm that the system is properly registered; and

3. Check the battery expiration date, if applicable.

ENCLOSURE 9

GUIDANCE FOR CONDUCTING SECURITY AUDITS

ENCLOSURE 9
VESSEL SECURITY AUDITS

1. Title 33, Part 101.105 (33 CFR 101.105) defines *audit* as "an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third party, ***intended to identify deficiencies, non-conformities, and/or inadequacies that would render the assessment or plan insufficient."*** 33 CFR 104.415, 105.415, and 106.415 provide requirements for the conduct of an annual audit of a regulated facility or vessel security plan.

2. The intent of the regulation and the purpose of an audit are to identify opportunities for improvement and to address nonconformities. The audit accomplishes this through the review of the operations of the regulated entity and the implementation of corrective actions which ensure regulatory compliance and preclude the recurrence of deficiencies. If, during the course of an audit, deficiencies and/or inadequacies are identified, then the security assessment and security plan of the regulated entity could have areas requiring improvement or revision. In this continuation of the audit and review of the security plans and assessments, more than one fix may need to be made. For instance, an identified security gap allowing unaccounted for persons to access a regulated entity would indicate a possible nonconformity in the implementation of the plan, or possibly point to deficiencies in the plan and assessment. It is the intent of the audit to make the security posture, and the underlying documentation, align and provide the tightest security appropriate for the situation.

3. Several opportunities exist for the auditor to analyze the effectiveness of the regulated entity in implementing their security plan. For example, review of quarterly drills, annual exercises, and corrective action following a deficiency or recorded security event (such as security incidents or breaches of security) provide an auditor the chance to see the plan operate and learn how it has been improved. An effective audit might include site visits during normal and other-than-normal hours, interviews with and observation of personnel performing security duties, review of and observation of security procedure implementation, as well verifying operability testing and planned maintenance of security equipment and ensuring that personnel are trained and proficient in their security duties.

4. During the audit, several documents could assist the auditor in his or her duties. Such documents include those associated with previously performed audits, drills, exercises, security incidents, compliance inspections, corrective action reports, and lessons learned.

5. 33 CFR 104.235(b)(8) requires a letter certified by the Company Security Officer or the Vessel Security Officer stating the date the audit was completed. While there is no requirement that an audit report be maintained, the sample audit report form on the next page of this NVIC may be used by an auditor to help organize their thoughts and their findings.

SAMPLE AUDIT REPORT FORM

NAME OF REGULATED ENTITY:

REPORT NUMBER:

AUDIT DATE(S):

DATE OF LAST AUDIT:

AUDITORS AND EVIDENCE THEY MEET 33 CFR 104.415(b)(4):

1.)
2.)
3.)
4.)
5.)

EXECUTIVE SUMMARY:

This section gives the auditor the opportunity to briefly describe their findings. Note: Requirements for the classification and protection of Sensitive Security Information is found in 49 CFR Part 1520.

DEFICIENCIES (D), NON-CONFORMITIES (N/C), PLAN INADEQUACIES (PI), OR AREAS FOR IMPROVEMENT (AFI) IDENTIFIED:

1.)
2.)
3.)
4.)
5.)

CURRENT SECURITY POSTURE:

This section gives the auditor the opportunity to describe NoteworthyFindings (NF), Observations (O), and Strengths (S).

NAME OF INVOLVED PARTIES FROM THE REGULATED ENTITY:

1.)
2.)
3.)

Audit Report Prepared by: _____ Company: _____ Date: _____

Audit Report Reviewed by: _____ Position:_____ Date: _____

Audit Certification Letter Attached to VSP by: _____ Date: _____