

## Circular 2017-21: Panama Flag Administration SSAS Guidance

### Overview

The Ship Security Alert System (SSAS) is part of the ISPS Code and is a system that contributes to the IMO's efforts to strengthen maritime security and suppress acts of terrorism and piracy against shipping.

Before the installation of the SSAS equipment, ship-owners or operators have to notify the Recognized Security Organization, which is responsible for the Safety Radio Certification and for the installation, inspection and testing of the SSAS, which will be done by an approved radio technician.

Panama flag administration issued the Merchant Marine Circular 133 in order to provide guidance on the issue. The highlights of the circular are analyzed below.

### SSAS TESTING by the Company

All the Companies must include the following e-mail addresses as recipient's address of the SSAS alerts / tests, on board the Panamanian Flagged vessels:

- [threat@amp.gob.pa](mailto:threat@amp.gob.pa) and/or
- [authorizations@segumar.com](mailto:authorizations@segumar.com)

A pre-authorization from Panama Maritime Authority to carry out SSAS Test or drill **is not required**. Panama Maritime Authority will only confirm the SSAS Test messages as requested by the Company or Master. In such cases, the word **"TEST"** will be clearly noted within the message.

The SSAS messages (alerts/tests) must include at least the following information:

- Name of ship
- IMO number
- Call sign
- Maritime Mobile Service Identity Number
- Date and time in UTC
- GNSS position of the ship (latitude and longitude)
- Course and speed

In case that the message received indicates the words **SSAS ALERT** or **SECURITY**, the PMA will require a confirmation about the status of the ship and crew.

When the Ship Security Alert System (SSAS) during a test transmits a false alarm, the Company or the Company Security Officer (CSO) must inform immediately to the Maritime Ships Security Department (PMA) in order to avoid any misunderstanding.

### Regulations for SSAS Test Message

According to Resolution No.106-107-DGMM dated October 9th, 2017 from January 1st, 2018, the annual SSAS TEST will be received through the use of an electronic platform for the Supply and Operation of the Ship Identification and Monitoring System.

The Company Security officer (CSO) designated by the operators and/or owners, must request from November 30th, 2017 access to the platform by email to the address [info@panama-ssas.com](mailto:info@panama-ssas.com), along with their access credentials to receive the instructions for the use of the platform.

The information submitted on the CSO Validation Form received and in the CSO online application will pass through directly to the electronic platform in order to obtain credentials. Operators and/or owners of the Panamanian registry vessels through the CSO have the responsibility to schedule, through the platform, the annual tests of **SSAS TEST** in a period **no longer than twelve (12) calendar months**. The confirmation message of the annual SSAS TEST should be retained on board as evidence of compliance with the MMC-133.

## Circular 2017-21: Panama Flag Administration SSAS Guidance

For ships to enter the Panamanian registry as of January 1st, 2018, they must schedule the first SSAS TEST through the use of the new platform, which must be verified by their RSO during the initial verification and from that date onwards, every 12 months as mentioned in previous paragraphs. In those cases, please be sure that the Company Security Officer designed by the Company Operator already has the Declaration of Company Security Officer duly endorsement by Panama Maritime Authority (MMC 206) in order to schedule the first SSAS TEST.

Only one annual SSAS TEST is mandatory. In case of vessels that perform more than one test and require a flag confirmation they should not schedule it through the platform, in those cases they also have to use the below SSAS TEST message information and send an email directly to [threat@amp.gob.pa](mailto:threat@amp.gob.pa).

All the Panamanian flagged vessels must keep the email address [threat@amp.gob.pa](mailto:threat@amp.gob.pa) (main) in their SSAS terminal. The use of [authorizations@segumar.com](mailto:authorizations@segumar.com) is optional.

### Annual SSAS Test Message

The SSAS TEST messages must include the following information:

1. TESTs must be sent via email, using ASCII, UTF-8 or ANSI encodings to the following address: [threat@amp.gob.pa](mailto:threat@amp.gob.pa) .
2. The name of the vessel must be written in closed capital letters and should appear exactly as it is written in the Navigation Documents.
3. The IMO number
4. The Mobile Maritime Vessel Identifier (MMSI) - 9 digits, which cannot be separated by spaces, dashes or other characters.
5. The Call Sign must contain between 4 and 7 digits and must appear exactly as it is written in the ship's registration patent.
6. The date of the test
7. The time of the test
8. The coordinates of the position of the vessel at the time of the SSAS test.
9. The heading of the vessel at the time of the TEST shall be expressed in degrees.
10. The speed of the vessel at the time of the TEST shall be expressed in knots.
11. Messages must include the word **"TEST TEST"**.

In case the message received does not contain the words "TEST TEST", the Panama Maritime Authority will request confirmation to the CSO about the status of the ship, the crew and thus, in this way rule out any case of false alarm.

For Further details please refer to PMA MMC-133.

All RSO's must verify in the initial verification that the SSAS system is working properly, performing a real TEST and sending it to [threat@amp.gob.pa](mailto:threat@amp.gob.pa) in order to confirm receipt.

### Confirmation Message of the Annual SSAS Test

SUSCCESFUL TEST when:

- The Maritime Ships Security Department confirms the reception of the same in the date scheduled in the Electronic Platform.
- The TEST message includes all the information described in the Merchant Marine Circular that will be issued for such purposes.
- The general ship data such as: name, IMO number, call signs and MMSI numbers are correct, as are the geographic coordinates and date received.

## Circular 2017-21: Panama Flag Administration SSAS Guidance

**FAILED TEST:** In the event that the test does not comply with the information above and shall be re-scheduled through the platform in accordance with what is established in the fifth paragraph of this Resolution.

**PENDING TEST:** In the event that the SSAS TEST cannot be carried out, and this must be notified by email to the account [info@panama-ssas.com](mailto:info@panama-ssas.com) 24 hours in advance, the reasons and the new date of programming through the platform.

In cases where the SSAS TEST cannot be performed due to technical problems of the equipment, it should be communicated to the email: [info@panama-ssas.com](mailto:info@panama-ssas.com).

In cases of noncompliance with these regulations the Panama Maritime Authority may impose the following sanctions:

1. The International Ship Security Certificate (ISSC) may be invalidated.
2. Additional audits of the ISPS Code may be authorized to vessels that demonstrate non-compliance with the provisions of this Resolution.

For more information about these new regulations and check the compatibility of the equipment please send an email to [info@panama-ssas.com](mailto:info@panama-ssas.com).

### SSAS Malfunctioning

In case of SSAS malfunctioning, an e-mail or a letter issued by the RSO indicating the exact date and place where the vessel will make the repair and programming of the SSAS equipment shall be submitted to the Maritime Ships Security Department to the e-mail address [isps@amp.gob.pa](mailto:isps@amp.gob.pa) or through any of the SEGUMAR Offices.

### Actions required

Ship managers and operators should stay alerted when operating in Piracy suspicious waters. All bridge personnel should be familiar with the use of SSAS for real threat warnings and for testing.

Additionally, ship managers and operators should:

- Provide every vessel with an effective **Ship Security Plan**
- Follow the **recommended maritime security transit corridors** in the high risk areas.
- Follow best practices (as required in **BMP-4**) and consider the use of embarked armed security
- Have their crews adequately trained and familiarized with any protective measures on board

### Further information

**SQEMARINE:** [Ship Security Plan](#)

**SAFETY4SEA:** [Panama MMC-133](#)