REPUBLIC OF CYPRUS

SHIPPING DEPUTY MINISTRY

Circular No: 35/2024

SDM 04.28.005.004.002
SDM 05.13.002

13 November 2024

All Registered Owners, Registered Bareboat Charterers,
Managers and Representatives of ships flying the Cyprus Flag

All Recognised Security Organisations (RSOs)

Subject: Maritime Security – Consolidated Instructions

I wish to inform you that the Shipping Deputy Ministry (SDM) hereby re- issues the Consolidated Instructions related to maritime security that had been announced via Circular No. 24/2015, as set out in the annexes to this Circular. You are reminded that full compliance with these requirements should be ensured.

2. All information and recent developments on maritime security are available on the official web page of the SDM under the title "Security" and you are kindly requested to consult this frequently for updates related to the implementation of the provisions of Regulation (EC) 725/2004, Chapter XI-2 of SOLAS 74 as amended and the ISPS Code.

Circular No. 24/2015 is revoked by this Circular.

This Circular must be placed on board ships flying the Cyprus Flag.

Dr. Anthony A. Madella
Director
for Permanent Secretary

cc: - Permanent Secretary, Ministry of Foreign Affairs
- Maritime Offices of the Shipping Deputy Ministry abroad
- Diplomatic and Consular Missions of the Republic
- Honorary Consular Officers of the Republic
- Cyprus Shipping Chamber
- Cyprus Union of Ship Owners
- Cyprus Bar Association

Encl.

ANNEX 1
COMMUNICATION WITH THE SHIPPING DEPUTY MINISTRY

1. Contact details

The Shipping Deputy Ministry (SDM) wishes to inform all parties that the contact details for maritime security issues concerning Cyprus flag ships are the following:

SHIPPING DEPUTY MINISTRY
Safety and Environmental Protection Directorate
Port State Control and Port Security Unit

Offices: Kyllinis Street, Mesa Geitonia, Lemesos, Cyprus
Postal Adress: P.O.Box 56193, 3305 Lemesos, Cyprus
Telephone: +357 25848100
Fax: +357 25848200
Emergency Telephone: +357 99377988

E-mail address for general matters on ISPS (ISPS matters other than Continuous Synopsis Record matters):

maritime.security@dms.gov.cy

E-mail address for Continuous Synopsis Record (CSR) (submission of ISPS C1, C2 and C3 forms as well as requests for issue and changes to CSR):

csr@dms.gov.cy

E-mail address for Ship Security Alerts (the email to which all ships' real security alerts to be transmitted from Cyprus flag ships):

ssas@dms.gov.cy

The SDM suggests that all e-mail messages are addressed to the dedicated e-mail addresses as stated above. E-mail messages should not be addressed to any of the personal email addresses of the SDM personnel unless it is requested by an officer of the SDM for a particular message to be sent to his / her personal e-mail address.

2. Downloads

All forms, including any future revisions, described in this Circular and other Circulars of the SDM related to maritime security are available to be downloaded from the web page of the SDM under "Documents / Application forms / Maritime Security - Forms", and "Technical / Security".

ANNEX 2
VERIFICATION AND CERTIFICATION

1. Recognised Security Organisations

The Classification Societies, listed below in alphabetic order, are authorized by the Republic of Cyprus as Recognised Security Organisations (RSOs):

- AMERICAN BUREAU OF SHIPPING (ABS);
- BUREAU VERITAS MARINE & OFFSHORE SAS;
- CHINA CLASSIFICATION SOCIETY;
- CROATIAN REGISTER OF SHIPPING;
- DNV AS;
- INDIAN REGISTER OF SHIPPING;
- KR (KOREAN REGISTER);
- LLOYD'S REGISTER GROUP LIMITED;
- NIPPON KAIJI KYOKAI GENERAL INCORPORATED FOUNDATION (CLASSNK);
- POLISH REGISTER OF SHIPPING;
- RINA SERVICES S.p.A..

The RSOs are authorized to review and approve ship security plans (SSP) of Cyprus flag ships, in accordance with ISPS-Code Part A, and the additional requirements of Cyprus.

The RSOs are also authorized to conduct all shipboard verifications (interim, initial, intermediate, renewal and additional verifications) and to issue the International Ship Security Certificate (ISSC) (interim and full term) on behalf of the Republic of Cyprus.

No additional authorization is required to be granted by the SDM for the conduct of any of the shipboard verifications.

2. Issuance of consecutive Interim ISSC

In case of a ship not be able to undergo an initial verification in order to be furnished with a full term ISSC prior the expiry of the interim ISSC, a written request must be submitted to the SDM, by the owner or the manager of the ship, for the issuance of a consecutive interim ISSC, along with the objective evidences, such as communication with the RSO of the ship, justifying the reasons for such a request.

The SDM, after examining the reasons and verifying that the purpose of the owner or the manager in requesting such certificate is not to avoid full compliance with SOLAS Chapter XI-2 and Part A of the ISPS Code, will approve in writing the issuance of a consecutive interim ISSC with a validity no more than 6 months from the date of expiry of the initial interim ISSC**. No consecutive interim ISSC should be issued by the RSO of the vessel prior the written approval of the SDM.**

3. Ship Security Plan Approval

Based on the experience gained so far and recent cases, RSOs are instructed:

- to approve SSP after the date of registration of a ship in the Cyprus Registry;
- to approve SSP after the date of interim security verification and certification of a ship and preferably at least three (3) months after the date of issuance of the interim International Ship Security Certificate (ISSC).

RSOs are hereby requested to upload on their on-line electronic database or send by email the letter of initial SSP approval as well as any future approvals of amendments to a SSP together with the ISSC and the relevant verification reports.

4. Failures of Security Systems during Verification and Certification Process

The SDM has observed that RSOs have issued or renewed ISSCs to Cyprus flag ships after verifications with failures identified and before their rectification. The SDM wishes to bring to all RSOs the provisions of MSC/Circ. 1097, Annex whereby it is clearly stated that:

> "Issue of the International Ship Security Certificate
>
> *10 The Committee concluded that a certificate should only be issued:*
>
> *.1 when the ship has an approved SSP; and*
>
> *.2 there is objective evidence to the satisfaction of the Administration that the ship is operating in accordance with the provisions of the approved plan.*
>
> *11 Certificates should not be issued in cases where minor deviations from the approved plan or the requirements of SOLAS chapter XI-2 and part A of the ISPS Code exist, even if these deviations do not compromise the ship's ability to operate at security levels 1 to 3."*

The SDM urges all RSOs to strictly apply the above mention provision and to follow the provisions of IACS Procedural Requirement No.24 Rev.1 entitle "Procedural Requirements for ISPS Code Certification" or any future revision.

No ISSC should be issued or renewed when failures are identified and no ISSC should be endorsed when major failures are identified during the relevant verifications unless appropriate measure /actions are taken by the ship to restore compliance. The RSO's attending auditor(s) shall verify the implementation of these measures prior the ship sails. In addition, depending on the nature and seriousness of the failure identified, a schedule for the implementation of preventative action may need to be agreed between the Company and the auditor to prevent recurrence. Additional audits may be carried out as necessary.

The RSOs should contact SDM, for further guidance and actions, in the following cases:

1. Failures identified during an ISPS initial or renewal verification cannot be rectified / resolved prior the ship's sails from the port /place of verification, and

2. Major failures identified during an ISPS Intermediate verification cannot be rectified / resolved prior the ship's sails from the port /place of verification.

Furthermore, the SDM has noticed that, in several cases, RSOs have classified and recorded on their audit reports failures as “observations”. Considering that an observation is defined as a statement of fact which if not corrected may lead to a failure in the future, the use of the described approach resulting in the non-rectification of identified deficiencies / failures. Based on the above the SDM does not accept or allow the use of the said approach / practice and all RSOs must take necessary actions to prevent reoccurrence in the future.

5. Monitoring the Implementation of Regulation (EC) 725/2004

The SDM in its effort to monitor the implementation of the European Regulation (EC) 725 / 2004 (ISPS Code) on Cyprus Flag Ships and establish a closer and better collaboration with the appointed RSOs that approve ship security plans and issue ISSC to Cyprus flag ships, wishes to continue participation during shipboard ISPS verifications carried out by all RSOs.

In this respect, surveyors of the SDM **may** participate during initial, intermediate, renewal and additional ISPS verifications which will be scheduled to be carried out on board Cyprus flag ships by the RSOs. Surveyors will attend ISPS audits at the following ports:

- All ports in the Republic of Cyprus.
- All ports in the Hellenic Republic.
- All ports in the Netherlands.
- All ports in the Federal Republic of Germany.

The scheduled date for ship board ISPS verification for each and every ship (together with details of the ship (name and IMO of the ship), type of verification, and contact details of attending surveyor must be forwarded to both the Limassol Head Office (via the dedicated email for maritime security) and the corresponding SDM Overseas Office as stated above. RSOs are kindly requested to send the information well in advance (as soon as the verification has been arranged with the owner/manager of the ship and at least four (4) working days in advance) in order to enable us to make the necessary arrangements for participation.

The SDM will notify you by email or telephone for those cases it intends to participate with its surveyors. It is noted that, the dedicated maritime security email address of the SDM as well as the contact details of its overseas offices, where information for shipboard verifications should be communicated, are available on the SDM website.

ANNEX 3
IMPLEMENTATION OF THE ISPS CODE

1. Language of the Ship Security Plan (ISPS Code, Part A, 9.4)

The Ship Security Plan (SSP) should be written in Greek or English and to any other languages designated by the Company as the command and the working languages on-board their ship.

2. Copies of the approved SSP and of any subsequent amendments thereto

The SDM requires each Company to have in the office from which the ship is operated at least one copy of the approved SSP (including any subsequently approved amendments thereto) relating to that ship. This copy of the SSP (and any amendments thereto) shall be protected from unauthorised access or disclosure.

3. SSP as part of the Safety Management System

In the interest of the national security of the Republic of Cyprus as well as of the other Contracting Governments and the need to protect the SSP from unauthorised access and disclosure, SSPs must NOT form or be part of safety management systems.

4. Interface with ships or ports that are not subject to the requirements of the ISPS Code and Regulation (EC) 725/2004

The SSP should include provisions to ensure that security is not compromised by any ship to port or ship to ship activity, with a port or a ship which are not subject to the provisions of the ISPS Code and Art. 3.8 of the Regulation (EC) 725/2004.

5. Changes to SSP (ISPS Code, Part A, 9.5)

Changes to a SSP must be applied only after these have been approved by the RSO that has approved the SSP and has issued the ship´s ISSC.

All items described under the provisions of the ISPS Code, Part A/9.4 must be firstly approved by the RSO of the ship prior to their implementation with the only exemption being the contact details of the CSO and alternate CSO (ISPS Code, Part A/ 9.4.14) provided that the approved SSP contains in the main text the duties of the CSO and his/her alternates (ISPS Code Part A/12) and that the contact details are attached to the SSP as an annex.

The SDM will only accept the above-mentioned arrangement provided that the ISPS C-1 form is submitted to the SDM prior to the implementation of the changes.

If changes of the CSO / alternate CSO details are not communicated to SDM in time and / or the SDM is unable to reach the CSO and or alternate CSO, these cases will be treated as non-compliances with the provisions of this Circular and will result to additional investigation by the SDM (i.e. additional ship board verification may be requested to be carried out by the RSO or additional shore-based verification may be requested to be conducted by either the SDM or the RO issuing the Document of Compliance of the company).

The following cases are considered significant, necessitating changes to the SSP plans, which must be submitted for approval prior to their implementation:

- When a ship has undergone a major conversion as defined by SOLAS 74 as amended.
- When any or all of the restricted areas have been changed.
- When new surveillance equipment and related equipment is installed on board for monitoring the security of the ship and these have not been included in the approved SSP.
- When procedures related to the SSP and actions taken when the ship is on security level 1, 2 and 3 are modified.
- When a ship is going to trade in areas that have not been covered by the ship security assessment.

6. Nomination of the Company Security Officer, his/her Alternate and the Recognised Security Organisation

The Company, bearing in mind the requirements of sections A/11.2, A/13.1 and paragraph B/13.1 of the ISPS Code, must designate Company Security Officer(s) (CSO(s)) and alternate CSO(s) for the ships it operates. Their names and contact details shall be identified in the SSP.

Persons who have satisfactorily completed an approved course based on IMO Model Course 3.20 on CSO, or who have attended a course based on the knowledge, understanding and proficiency (KUP) as stated at the Annex of the MSC Circular 1154, are considered to have met the above-mentioned requirements for service as a CSO and alternate CSO.

Any Designated Persons (DP) (section 4 of the ISM Code) and any alternate DP, may also be designated as a CSO or alternate CSO, provided the requirements of sections A/11.2, A/13.1 and paragraph B/13.1 are met. In such a case, it is the Company concerned which has to ensure that such a person can adequately and efficiently perform both functions.

The name and contact details of the CSO and the alternate CSO must be communicated to the SDM using the ISPS C-1 form and any changes relating thereto. The form must be clearly typed and signed prior to its submission. When more than one CSO and his/her alternate is nominated by a company, then for each such nomination separate forms must be used.

The ISPS C-1 form is also used to notify the SDM of the nomination of the RSO of the ship and any changes relating thereto.

Whenever there are any changes of the contents of ISPS C-1 form, the Company must promptly inform the SDM by submitting an updated form.

In case of changes to the CSO and/or the alternate CSO, the Ship Security Plans (SSP) must be amended accordingly to contain the details of the new CSO and/or alternate CSO.

The ISPS C-1 forms and relevant notifications to the SDM, must be available for examination during shore-based verifications of the safety management system of the

Company by the Recognised Organisation (RO) issuing the Document of Compliance (DoC) of the Company as per the provisions of the International Safety Management (ISM) Code.

7. Ship Security Officers and alternate Ship Security Officers

All Cyprus ships are required to have a Ship Security Officer (SSO) and an alternate SSO. The SSO and alternate SSO must be identified in the SSP by rank. In this way the SSO and the alternate SSO can be identified through a cross reference to the Crew List of the ship at the time. In this manner, the need to submit amendments to the SSP for approval, as a result of shipboard personnel changes, is avoided.

Any member of the ship's personnel, including the Master, may be designated as the SSO or as an alternate SSO provided he has the required training and understanding of the duties and obligations of the SSO or of the alternate SSO.

All SSOs and alternate SSOs on board Cyprus flagged vessel must have a certificate issued by this Administration or by a country whose certificates are recognised by the Republic of Cyprus, in accordance with regulation VI/5 of STCW 78 as amended. A list of countries whose certificates are recognised and a list of countries which are not issuing such certificates but they accept the certificates issued by training schools is available on the web page of the SDM under "Seafarers, Training and Certification".

The SDM has issued additional instructions on the Manila Amendments of the STCW that are applicable as from 01 January 2012. The amendments are related to the Regulation VI/6 of the STCW 78 as amended on:

- Security awareness training for the crew without security duties; and
- Security awareness training for crew with security duties without SSO certificate.

All seafarers, on board a Cyprus flagged ship, without SSO certificate, must hold one of the above-mentioned certificates as required by his/her appointment on board.

Owners and Managers of Cyprus vessels are reminded that more information and applications for the issuance of the aforesaid certificates may be obtained from the Seafarers Division of the SDM.

8. Conducting Ship Security Exercises (ISPS Code, Part B/13.7)

The Company should ensure that, for its entire fleet, a ship to shore exercise is carried out involving one (1) ship (under Cyprus flag) or more if so wished, at least once every calendar year, with no more than eighteen (18) months between exercises.

Each year, a different ship (if one ship is chosen to conduct the exercise every year) must be selected when conducting the ISPS exercises.

Furthermore, the scenario of the exercise must be different each year as per the relevant provisions of the approved SSP and paragraph 8.9 of Part B of the ISPS Code.

Prior the conduct of any exercise, the SDM must be notified in writing by the CSO or the alternate CSO, at least **three (3) working days** in advance using the **“**Reporting the Conduct of an ISPS Exercise” form.

The involvement of the SDM at any security exercise will be limited to the testing of efficient communication with the CSO and or alternate CSO and the successful transmission in real mode of a Ship Security Alert (SSA) (if this is included in the exercise scenario), during normal working hours of the SDM. The SDM will confirm the reception of SSA provided that the activation in real mode was announced and requested prior to the conduct of the exercise.

Upon completion of every exercise, the CSO or alternate CSO must submit a brief evaluation report regarding the conduct of the exercise using the “Reporting the Evaluation of an ISPS Exercise” form.

Exercises conducted with ships flying other than Cyprus Flag do not fall under the provisions of the present Circular as the SDM has no access to the ship security plans of the ships and cannot be involved in the process of establishing and confirming proper communication with the ship using the SSAS.

The SDM wishes to limit the documentation and the required information only to the two above-mentioned forms and will only request the submission of additional documents when deemed necessary.

Any internal communication, carried out between the ship and the shore-based personnel of the company, is not necessary to be submitted or communicated to the SDM.

If exercises are not communicated to SDM, these cases will be treated as failure of the ship and the company in question to comply with the provisions of this Circular and might result to an additional investigation by the SDM (i.e. additional shipboard verification may be requested to be carried out by the SDM or RSO or additional shore based verification may be requested to be conducted by either the SDM or the RO issuing the Document of Compliance of the company).

The records of exercises, including information to be submitted to the SDM, must be available for examination during shore-based verifications of the safety management system of the Company by the RO issuing the DoC of the Company as per the provisions of the ISM Code.

Finally, the CSO’s and / or alternate CSO’s are reminded that all findings and lessons must be communicated to the entire fleet of the company (if more than one ship under Cyprus flag exists in the fleet).

9. Ship Security Alert System (SSAS)

9.1 Requirements for the SSAS

In accordance with Regulation 6/ XI-2, all ships that are referred to in Regulation 2/ XI-2 shall be provided with a Ship Security Alert System (SSAS). The SSAS shall meet the performance standards laid down by the Resolution MSC. 147 (77), MSC/Circ. 1072 and MSC.1/Circ 1190.

The Ship Security Alert System shall be programmed to transmit the following information:

- Name of ship;
- IMO Ship Identification Number;
- Call Sign;
- Maritime Mobile Service Identity (MMSI);
- GNSS position (Latitude and Longitude) of the ship; and
- Date and time (UTC) of the GNSS position.

Additional information such as the name and contact phone number for the CSO (and alternate CSO) may be included if the SSAS is capable of such programming but this additional information is not mandatory.

The SSAS, when activated in real mode, must transmit a ship to shore security alert to the ship management company as well as to the SDM, to the email address that is dedicated to receive such alerts. The email address is: ssas@dms.gov.cy

9.2 Commissioning and testing of the SSAS

The SDM urges ship owners, ship managers and operators to exercise extreme care when commission the SSAS on board a Cyprus flag vessel to avoid false activation of the system.

It is advisable that when a technician is attending the vessel or if for any reason the system will be activated in real mode, the SDM is notified in writing at least 24 hours in advanced providing details of the ship (name, IMO number, Call Sign and MMSI), date and time of activation and the reason for activating the SSAS. All notifications must be transmitted to maritime.security@dms.gov.cy

The SDM requires an activation in real mode of the SSAS to be carried out as soon as the system has been initially commissioned. Thereafter, the SSAS shall be tested (activation of the system in real mode) **annually,** either as a part of the annual ship security exercise or independently, i.e. once between the calendar months January to December.

The SSAS must also be tested (activation of the system in real mode) when a ship changes management company or service provider.

The SDM will only confirm reception of a ship security alert provided that this was requested prior to the activation of the SSAS (in real mode) providing details of the ship (name, IMO number, Call Sign and MMSI) and date and time of activation. Confirmations will be carried out by the SDM during normal working hours of the SDM.

The SDM does not wish to receive security alerts due to the activation of SSAS in test mode, as a part of the routine testing of the system between the ship and its company. The SDM will not confirm reception of such test messages.

The records of real SSAS, including confirmations from the SDM, must be available for examination during shore-based verifications of the safety management system of the Company by the RO issuing the DoC of the Company as per the provisions of the ISM Code.

9.3 False activation of the SSAS

If for any reason the SSAS is activated in real mode and a real alert is transmitted, the CSO or his / her alternate must immediately notify the SDM in writing stating the details of the ship (name, IMO number, Call Sign and MMSI) and the reason for such activation.

9.4 Real activation of the SSAS due to a threat

The SDM must be informed immediately of a REAL SSAS activation due to a threat by the CSO and or alternate CSO of the ship on the dedicated 24/7 telephone number: + 357 99 377 988.

The CSO or his alternate, after they have confirmed that the ship is under threat, must also provide to the SDM, the information stated on the "ISPS security incident report" Form.

9.5 Ships deleted from the Registry of Cyprus Ships

When a ship is deleted from the Registry of Cyprus Ships, the Company shall immediately make all necessary arrangements for the reprogramming of the SSAS.

9.6 SSAS types and models accepted to be placed on board Cyprus flag ships

The SSAS types and models accepted by this Deputy Ministry are appended on the web page of the SDM under Technical / Security / Security Alert Systems.

9.7 Records of SSAS testing during audits carried out by RSOs

RSO's are requested to examine the records SSAS activation and testing being kept on board ships during the ship board ISPS verifications (interim, initial, renewal or additional).

Records of SSAS activation and testing may also be verified during the initial, periodical or renewal surveys of the Cargo Ship Safety Radio Certificates (CSRC) and the initial or renewal surveys of the Passenger Ship Safety Certificates (PSSC).

10. Security Incidents

When a security incident occurs on-board a Cyprus flag ship, the CSO or the alternate CSO must inform the SDM, the soonest possible, using the "ISPS security incident report" Form.