

Commonwealth of Dominica**Office of the Maritime Administrator**

TO: ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS AND AUTHORIZED CLASSIFICATION SOCIETIES.

SUBJECT: International Ship & Port Facility Security Code (ISPS Code)

REFERENCES:

- (a) **Maritime Regulation 2.35,**
- (b) **International Ship and Port Facility Security Code,**
- (c) **SOLAS 74 Chapter V Regulation 19,**
- (d) **SOLAS 74 Chapter XI-1 Regulations 3 & 5,**
- (e) **SOLAS 74 Chapter XI-2,**
- (f) **International Safety Management Code IMO Resolution A.741(18),**
- (g) **IMO Resolution MSC.104 (73),**
- (h) **SOLAS 74 Chapter IX, Management for the Safe Operation of Ships,**

PURPOSE:

This Notice provides notice and guidance to the owners, operators, and masters of Commonwealth of Dominica ships concerning the Administration's requirements for compliance with the International Ship & Port Facility Security Code (ISPS Code). This guidance is designed to describe how Companies operating Commonwealth of Dominica ships can gain Commonwealth of Dominica International Ship Security Certification. It also contains the Administration's policies and interpretations regarding application and implementation of the ISPS Code part A, and incorporation of the relevant sections of Part B.

The National Requirements are not intended to be all-inclusive or to prohibit a Company from incorporating procedures, processes or other items that go beyond the ISPS Code, when developing or implementing the Ship's Security Program on board their vessels. Questions regarding the ISPS Code should be referred to the:

1 of 18

Commonwealth of Dominica Maritime Administration
Office of the Deputy Administrator for Maritime Affairs
32 Washington Street
Fairhaven, Massachusetts 02719
e-mail: edawicki@dominica-registry.com

1. APPLICABILITY:

This Notice is applicable to the following Commonwealth of Dominica ships engaged on international voyages:

- Passenger ships, including high-speed passenger craft;
- Cargo Ships, including high speed craft, of 500 Gross tonnage and Upwards;
- Cargo Ships, including high speed craft, of 100 Gross tonnage and Upwards traveling to US waters;
- Self Propelled Mobile offshore drilling units.

Where applicable specific equipment requirements for specific classes or types of ships are spelled out elsewhere in these instructions:

2. DEFINITIONS:

Definitions have been taken from the ISPS Code Part A, Paragraph 2 and SOLAS Chapter XI-2, Regulation 1. Where necessary, Commonwealth of Dominica interpretations have been added in *italics*.

2.1 Administration:

The Office of Deputy Administrator for Maritime Affairs
Commonwealth of Dominica
32 Washington Street
Fairhaven, Massachusetts 02719

2.2 Company:

The owner of the ship, or the organization, or person such as the Manager, or the Bareboat Charterer, assuming the responsibility for operation of the ship from the ship owner, and when assuming such responsibility has agreed *in writing* to take over all the duties and responsibilities imposed by the ISM Code. Companies are urged to use the Commonwealth of Dominica Maritime Registry ISPS Code Ship Assessment Template and the Ship Security Plan Template for a streamlined certification process. Companies using other systems may find delays if the plans are not formatted to the CODMR standards.

2.3 Commonwealth of Dominica Security Auditor:

A Commonwealth of Dominica Nautical inspector who has been trained as a security auditor and appointed by the Administration to conduct security verifications of Commonwealth of Dominica flag ships. The Commonwealth of Dominica security auditor will be issued an identification card stating the Inspector is qualified to perform security verifications on behalf of the Administration.

2.4 Recognized Security Organization (RSO):

An IACS member Classification Society, or Maritime Institute with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized by the Administration to carry out security verifications and certification of Commonwealth of Dominica ships. Dominica Regional offices have approved auditors throughout the world.

2.5 Security Consultants:

Organizations, which may perform threat assessments, vulnerability assessments, develop security plans and/or provide training to CSOs and SSOs.

2.6 Port Facility Security Officer (PFSO):

The person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with ship security officer and company security officer.

2.7 Company Security Officer (CSO):

The person designated by the Company for ensuring that a Ship Security Assessment is a carried out; that the ship security plan is developed, submitted for approval and thereafter implemented and maintained and for liaison with the port facility security officer, ship security officer and the Administration.

2.8 Ship Security Officer (SSO):

A senior officer on board the ship, who if not the Master, is accountable to the master and designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer, port facility security Officer and the Administration.

2.9 Security Level 1:

The level for which the minimum appropriate protective security measures shall be maintained at all times.

2.10 Security Level 2:

The level for appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of security incident.

2.11 Security Level 3:

The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.12 Ship Security Assessment or Security Assessment:

A process of defining the threats, and examining the ship's vulnerability to attack in order to design an effective security plan.

2.13 Ship Security Plan:

A plan developed *for each vessel in the fleet* by a competent Company Security Officer or a security consultant to ensure the application of measures on board the ship designated to protect persons on board, cargo, cargo transport units, ship's stores or ship from risks of a security incident.

2.14 Verification:

Evaluation of the Security Plan implementation on board a Ship by Commonwealth of Dominica security auditor or by RSO to determine compliance with the ISPS Code.

3. COMPLIANCE GUIDANCE:

3.1 Compliance with the Code will become mandatory on 1 July 2004. By this date every ship to which the Code applies must have:

- A Company Security Officer;
- A Ship Security Officer;
- Implemented an approved Security Plan;
- Installed or have plans for the installation of a Security Alert System;
- Installed or have plans for the installation of AIS;
- The IMO Number marked on the vessel or plans for marking the vessel, and
- Have available a Continuous Synopsis Record (CSR).

3.2 Recommended time-line for implementation:

- Before 1 July 2003, the Company should have a trained Company Security Officer;

- Before 1 October 2003, the Company should have plans for selecting and training Ship Security Officers;
- Before 1 February 2004 the Company should have:
 - Completed the initial vulnerability assessments, and
 - Drafted a security plan for each vessel.

- Before 1 May 2004, Ship Security Plans should be submitted to the Administration for approval;
- By or before 1 April 2004, the trained Ship Security Officer should be onboard and the approved ship security plan should be implemented. The verification and certification should be scheduled with the Commonwealth of Dominica security auditor or RSO.

3.3 Training of CSO and SSO:

The company is responsible for ensuring that the Company Security Officer and Ship Security Officer receive the appropriate training and that they obtain documentary evidence, which demonstrates satisfactorily education of ship security training. If determined by the company as the best course of action the CSO may also attend a “train the trainer” course so he can train the Ship’s Security Officers in their duties.

3.4 Using a Security Consultant:

Companies with adequate resources may decide to train or hire people to develop the required ship security expertise within their organization. Such staff will draft their own Ship’s Security Plans and conduct the Ship Security Assessments. However, this is may not be an effective method for companies who do not have the resources to support hiring or setting aside specific staff to develop the company’s security program. For such companies, it is recommended to consider the use of security consultants to assist with ISPS implementation. The Administration has examined documents and records as well as conducted interviews of a number of security consultants who offer services to assist companies with developing a security program that meets the ISPS Code. We recommend that before contracting with a security consultant you should ensure that the consultant has contacted the Administration. A company choosing to use security consultants should verify the validity of the information provided by the consultants and their ability to assist the company to comply with the ISPS Code requirements. (ISPS Code Part B paragraph 8 and 9).

3.5 Manning:

As part of the vulnerability assessment, the company should take into account any additional workload, which may result from implementation of the ship security plan and ensure that the ship is sufficiently and effectively manned. The company should consider the need to use contracted personnel for short periods of time to augment the ship's force in order to provide sufficient security.

3.6 Ship security plan template:

We recommend that the Ship's Security Plan be developed using the Commonwealth of Dominica Model Ship Security Plan Guidance and Security Plan Template. This template is designed to be a starting point. Other guidance may be used to develop the plans and to perform the Security Assessment. The security plan should be tailored to suit the needs and culture of your management system. However, to facilitate review, we do ask that the plan developers follow the index provided in the template. The Ship Security Plan Template and Guidance are available to every company security officer and designated person ashore managing a Commonwealth of Dominica flag vessel upon request. The guidance and template will continue to be modified as we gain experience.

3.7 Verification Audits and Certification:

The Administration is taking an active role in the security of ships flying the Commonwealth of Dominica Flag. We will be directly involved in the ISPS Code implementation and will carry out verifications on Commonwealth of Dominica flag ships. However, we also realize that there are clients that may prefer to use a RSO. A company can choose whether to have the Administration or the RSO to conduct the verifications. Companies choosing or interested in using the Liberia security auditors should contact the Administration or the local Commonwealth of Dominica security auditor.

3.8 ISPS and the ISM Code

Although it is not a requirement, the company should contemplate incorporating the shipboard security requirements into the Company's Safety Management System (SMS).

The Safety Management system should address the following:

- Define the security duties and responsibilities for the Company Security Officer, the Ship's Security Officers and the crew;
- Discuss who will be responsible for organizing security drills and exercises;
- Contain procedures for immediately reporting any noncompliance with the ISPS Code, threats and security incidents to the Administration;
- Defined the maintenance requirements for the Security Equipment;
- Provide for the logging of actions or measures taken to rectify deficiencies and non-conformities noted during Security Assessments and notification of the Administration and the RSO of any corrective actions taken;

6 of 18

- State the company will provide the support necessary to the company security officer, the master and/or the ship security officer to fulfill their duties and responsibilities in accordance with chapter XI-2 and the ISPS Code.

3.9 Part B as Mandatory:

While the Commonwealth of Dominica Administration has not mandated compliance with applicable sections of ISPS Code Part B, companies are advised that Port State Control Authorities in the United States and the European Union may require mandatory compliance with Part B. If a vessel meets the requirements of the applicable sections of Part B, then the Administration will issue an Annex to the ISPS Certificate indicating such compliance in order to facilitate vessel operations. Vessels that desire such an Annex to the ISPS Certificate shall contact the Administration.

3.10 Master Authority:

The Commonwealth of Dominica Maritime Law defines the Rights and Duties of the Master. The Administration also acknowledges the importance of IMO Resolution A.443 (XI), "Decisions of the Shipmaster with regard to Maritime Safety and Marine Environment Protection". The Ship's Security Plan shall incorporate the elements of both A.443 (XI) and the National Requirements to ensure the Master's authority on board the ship. Therefore, any system of operational control implemented by Company shore based management must allow for the Master's absolute authority and discretion to take whatever action he/she considers to be in the best interest of passengers, crew, and the cargo.

4. COMMONWEALTH OF DOMINICA NATIONAL REQUIREMENTS:

4.1 Compliance Monitoring:

Compliance with the Code will be closely monitored and enforced by the Administration. Ships that fail to comply with the ISPS Code will be considered in violation of SOLAS and may be prevented from trading.

4.2 Designation of Company Security Officer:

The owner of each Vessel must provide the Office of the Deputy Commissioner with the name, address, telephone, fax, email, telex numbers and after office hours contact information of the individual(s) in their Company who have been designated as the Company Security Officer.

4.3 Selecting a Ship Security Officer:

The Company should designate at least one of the senior officers onboard to perform the Ship Security Officer duties. The individual selected should be an experienced member of the crew and shall be trained to fulfill his duty.

4.4 Conducting the Security Assessment:

The Company may use their Company Security Officer, other trained personnel or security consultants to conduct the on-scene Security Assessment. Personnel conducting Security Assessments shall be independent of the activities being assessed unless this is impracticable due to the size and the nature of the Company or of the ship. Specifically, the person conducting the Ship Security Assessment should not be any of the officers or crewmembers permanently assigned or serving onboard the ship.

4.5 Ship Security Assessments:

(ISPS Code Part A paragraph 8) 4.5.1 The Ship Security Assessment is an essential and integral part of the process of developing and updating the ship security plan. 4.5.2 The Ship Security Assessment shall include an on-scene security survey, which incorporates but is not limited to the following elements:

- Identification of existing security measures, procedures, operations;
- Identification and evaluation of key ship board operations that need protection;
- Identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- Identification of weaknesses, including human factors in the infrastructure, policies and procedures. 4.5.3 The Ship Security Assessment shall be documented, reviewed, accepted and retained on board the ship and with the Company.

4.6 Drafting the ship security plan:

The Company may choose to create the Ship's Security Plans using their trained Company Security Officer, or they may use a Security Consultant. When using a consultant the company should make sure the plan reflects the company's security and that the companies policies and practices that are achievable. Commonwealth of Dominica security auditors and RSOs cannot assist the Company with developing their Ship Security Plans if they intend to conduct the ship's Verification on behalf of the Administration.

4.7 Fleet Plans and Sister Ships:

Each vessel shall have an individual plan tailored to its Security Assessment. However, there will be information in each ship's plan that will be the same for all of the ships in the company's fleet, for vessels on the same trade route and for sister ships operating in the same trade. The Security Assessment for the first ship can be used as a model for each of

the other ships engaged in the same trade on the same routes. In such a case only the ship's specific variations need be addressed during the on-scene Security Assessment.

4.8 Declaration of Security:

The Ship's Security Plan shall reflect the Administration's requirement that the Ship's Security Officer shall complete a Declaration of Security as described in the ISPS Code Part A paragraph 5 and *when deemed necessary by the Master or SSO*.

The Administration requires the completed Declaration of Security to be kept onboard for *one year* or for the last 10 Ports visited, whichever comes first.

4.9 Language:

All ship Security Plans shall be written in English and the working language of the crew if other than English.

4.10 Security plan approval:

All plans will be approved by the Administration. The company shall submit a single hard copy of each ship's security plan to the Administration for approval. All plans shall include the current Security Assessment that forms the basis of the plan, or the amendments.

4.11 Sending the Security plan in a secured manner:

The plan shall be mailed to the following:

Commonwealth of Dominica Maritime Administration
Office of the Deputy Administrator for Maritime Affairs
32 Washington Street
Fairhaven, Massachusetts 02719
e-mail: edawicki@dominica-registry.com

A courier service, which has a tracking facility, must be used. It shall be sent in a sealed envelope or box inside the shipping container supplied by the courier service. The company sending the Ship's Security Plan shall send an email or fax to edawicki@dominica-registry.com or 508-992-7120 stating the date the plan was sent, the contact information for the courier service and the tracking number. The Administration will follow a similar process in returning the plan.

4.12 Alterations to the approved plan:

When approving the Ship Security Plan, the Administration will determine which sections of the plan, if any that will not require prior approval by the Administration. Any other amendments to the approved security plan or changes to installed security equipment identified in the approved plan shall not be implemented without approval. Such changes shall be at least as effective as those measures prescribed in chapter XI-2, Part A and the applicable sections of Part B of the ISPS Code. The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration shall be clearly documented in the plan. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate).

4.13 Electronic Format:

The Ship Security Plan may be maintained by the company and aboard their ships in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. The Company must send one hard copy for approval accompanied with the electronic version.

4.14 Security of the Plan:

The Plan shall be protected from unauthorized use or exposure. The Company Security Officer and the Ship's Security Officer are responsible for the security of the plan. The Company Security Officer will determine which parts of the plan shall be available to the crew and which items are to be kept confidential, taking in consideration the following:

- Identification of the restricted areas;
- Procedures for responding to security threats;
- Procedures for responding to security instructions from contracting governments or administrations when setting security level 2 and level 3;
- Duties of shipboard personnel assigned security duties;
- Procedures for ensuring the inspection, testing, calibration and maintenance of security equipment on board;
- The location of the Ship Security Alert activation switches;
- Guidance or instructions on the use of the ship security alert system, including testing activation, deactivation and resetting and the methods for limiting false alerts.

4.15 Company Security Exercises:

The Administration may want to participate in your Company Security Exercises to evaluate the effectiveness of the Plan and the interaction of the Company Security Officer with the Security Plan. The Company Security Officer, when requested by the Administration, will provide the following information:

10 of 18

- The date of the exercise;
- The name of the Ship;
- The place where the exercise will take place, and
- The type of exercise.

4.16 Planning the Verification:

The Commonwealth of Dominica security auditor or the RSO will prepare the verification plan in consultation with the Company Security Officer. 4.16.1 The verification plan shall be sufficiently flexible to permit changes based on information gathered during the verification. 4.16.2. The verification plan shall include the following elements:

- Objectives and scope;
- Findings after review of the Security Plan;
- Identification of Company and Ship Security Officer;
- Identification of reference documents such as the applicable Code, Threat Assessment, Ship Security Assessment;
- Identification of auditor's qualifications;
- Dates and places where the verification will be conducted;
- The expected time and duration for each activity;
- The schedule of meetings to be held with the Company; and Confidentiality requirements. The Verification plan shall be part of the report, which will be provided to the Administration for final review.

4.17 Verification:

Only the Commonwealth of Dominica security auditor or the RSO are approved to conduct verifications on behalf of the Administration as follows:

- The Commonwealth of Dominica security auditor or the RSO cannot provide ISPS Code verification on a Commonwealth of Dominica ship in which any of its subsidiaries or commonly owned affiliates have performed Ship Security Assessments or prepared ship security plan for that ship;
- The company must contact the Administration or RSO to arrange for the initial verification. Failure to conduct the initial verification will be considered a violation of SOLAS and the ship may be prevented from trading;
- No verification shall be conducted if the document review of the Ship Security Plan indicates that the Ship Security Assessment conducted by the Company Security Officer or his contracted Security Consultant does not meet the requirements of the ISPS Code;

- The implementation period required before security Verification can be carried out should be 2 months.

4.18 Minor Deficiencies and Additional Verifications:

4.18.1: An ISSP Certificate may be issued despite the identification of minor ISPS Code deficiencies. Minor deficiencies identified by the Commonwealth of Dominica security auditor or RSO shall be reported to the Administration and documented as ISM Code non-conformities. Failure to correct the deficiencies within the specified time limit may result in the withdrawal of the ISSP Certificate and the Safety Management Certificate.

4.18.2: The Administration retains the right to conduct verification and inspection activities independent of or in concert with those of a RSO in order to verify proper implementation, application, and enforcement of the provisions of the ISPS Code.

4.19 Certification:

An International Ship Security Certificate (ISSC) shall be issued to each ship following a satisfactory Verification either by the Commonwealth of Dominica security auditor or a RSO working on behalf of the Administration.

4.19.1: The ISSC will not be issued until all major deficiencies in the implementation or the plan itself have been rectified.

4.19.2: The ISSC may be issued for a period of up to five years. It may be issued for a shorter period of time if the Company wants to harmonize the certificate with the SMC.

4.19.3: The validity of the Certificate is subject to at least one intermediate verification (by the RSO or the Administration) between the dates of second and third anniversary of the issuance of the ISSC. If the Certificate is issued for a period of less than three years the verification will be conducted upon the renewal assessment and an intermediate verification will not be required.

4.19.4: The Company is responsible for conducting an internal security audit each year on each ship to assess the functioning and effectiveness of the Ship Security Plan on board. This can be done in concert with the internal ISM audit.

4.19.5: Re-issuance of the International Ship Security Certificate is contingent upon the satisfactory verification of the effectiveness of the Ship's Security Plan in meeting the objectives specified by the ISPS Code.

4.20 Interim Certification:

4.20.1: Interim Commonwealth of Dominica International Ship Security Certificates may only be issued to the following vessels, after 1 July 2004, provided the Administration or RSO acting on behalf of the Administration is satisfied the ship is in compliance with the ISPS Code:

- New ships on delivery;
- Existing ships on reactivation;
- Transfer from another Flag, or
- A Company takes on responsibility for the operation of a ship which is new to the Company.

4.20.2: The Interim International Ship Security Certificate may only be issued by the Administration or the RSO after the following verifications by the Commonwealth of Dominica security auditor or RSO respectively:

- The Ship has an Approved Security Plan on board;
- The Company Security Officer has been designated;
- The Ship Security Officer has been designated;
- The Master and relevant senior officers are familiar with their Security Duties;
- The crew has received security training before the vessel gets underway;
- The required records have been started and will be maintained;
- Security instructions which the Company has identified as essential to be provided to the Master prior to the Vessel's first voyage under Commonwealth of Dominica flag have, in fact, been given to the Master; and
- There is a plan to conduct a full Verification within three months.

4.20.3: Prior to the expiration of the Interim International Ship Security Certificates, the RSO or the Administration should issue full term International Ship Security Certificates upon satisfactory evidence that the Ship's Security Plan has been implemented on board the ship.

4.20.4: Vessels unable to comply with the two months implementation period as specified in 4.17 due to change of ownership or management shall contact the Administration. Determination of interim certification prior to 1 July 2004 will be made on a case-by-case basis.

4.21 Exemptions and Dispensations:

All vessels to which the ISPS Code applies must obtain certification prior to 1 July 2004. The Administration will not grant exemptions in order to extend this deadline. The Administration will not consider issuing dispensations. Companies are advised that Port State Control Authorities may prohibit entry into port any vessel with such a dispensation.

13 of 18

5. NONCOMPLIANCE WITH THE ISPS CODE

5.1 Certificate Withdrawal:

ISPS Certificates may only be withdrawn at the determination of the Administration. Cause for certificate withdrawal may include but is not limited to the following deficiencies:

- Failure to coordinate and conduct the periodic or intermediate verifications;
- The information on the CSR is not correct;
- The Company's Security Officer fails to ensure compliance of a vessel;
- The Ship's failure to maintain its Ship's Security Plan in compliance with requirements of the ISPS Code;
- Deviations or defects related to the ISPS Code requirements which remain uncorrected beyond their due date, and
- The recommendation of the RSO or Commonwealth of Dominica Security Auditor based upon evidence of the vessel's noncompliance with the code.

5.2 Appeals:

In the event a Company disagrees with a determination made by the Commonwealth of Dominica security auditor or the RSO, the Company Security Officer may make a direct appeal to the Administration. The final determination will be based upon both the substance of the appeal and the recommendations of the Commonwealth of Dominica security auditor or the RSO.

6. Alternative Security Agreements:

At the request of the vessel's operators the Administration will conclude Alternative Security Agreements with other Contracting Governments for vessels engaged upon limited short International voyages, usually on fixed routes between ports that must also be party to the agreement. As part of the agreement, Liberia or one of the other contracting governments signing the report shall agree to inform other Contracting Government which may be affected by providing a notice to the appropriate subcommittee at IMO. In no case, shall such agreement compromise the level of security of other ships, port facilities not covered by this agreement. Ships covered by such an agreement, may not engage in ship-to-ship activities with ships not covered by said agreement. Such agreements shall be reviewed by this Administration annually or earlier if the need arises and shall be reviewed by all parties at least every five years. It is the vessel's operator responsibility for working with the other contracting government to develop the first draft of the agreement for signature.

7. PORT AND COASTAL AUTHORITIES:

7.1 Interaction:

The Company Security Officer and Ship's Security Officers are encouraged to contact the Port Facility Security Officer and develop a close working relationship.

7.2 Differences in the Security levels set:

If the ship is at a security level, which is different from that of the Port or Coastal State Authority's, then the ship will set the higher security level of the two. If the Ship Security level is higher than the Port's Security level the Ship Security Officer will notify the Company Security Officer. The CSO should provide this information to the PFSO with any background information that he has available.

7.3 Report of Port Facility Security defects:

When a Ship Security officer has determined that there is a problem with the port's Security Program, he is to report the problem to the Master. Once the Master determines that this is a defect that cannot be resolved with the local port authorities, he will report to the Company Security Officer. The CSO shall contact the Administration if assistance in obtaining a resolution is needed.

7.4 Report of Ship Security defects:

When a Port State inspector has determined that there is a problem with the Ship's Security Plan or the implementation of the plan on board a ship, the Master is to report the problem to the Company Security Officer. The CSO shall notify the Administration.

8. TECHNICAL AND EQUIPMENT REQUIREMENTS:

8.1 Ship Identification Number:

(SOLAS Chapter XI-1 Regulation3): The ships identification number (IMO number) shall be permanently marked on the vessel in accordance with the regulations. It will include the letters IMO in front of the number (IMO1234567).

8.1.1: The permanent marking will be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting color.

8.1.2: The markings shall be made by raised lettering or by cutting it in or by center punching it or by any other equivalent method that ensures the marking is not easily expunged.

8.1.3: On ships constructed of material other than steel or metal, the Administration shall have to approve the method of permanently marking.

8.1.4: If the number has been marked on the hull and one of the transverse bulkheads before these requirements were issued and is still in compliance with the ISPS code it will be accepted to the Administration.

8.2 Automatic Identification System (AIS):

All Commonwealth of Dominica Flag Ships engaged in international voyages are required to have an Automatic Identification System installed in accordance with SOLAS Chapter V Regulation 19.2.

8.2.1: The AIS Equipment installation shall be approved by the vessel's Classification Society or by the Administration by:

Type of vessel Compliance date:

- Passenger Ships Not later than 1 July 2003;
- Tankers of 500 GRT and upwards Not later than first safety equipment survey on or after 1 July 2003;
- Ships other than Passenger and Tankers of 300 GRT but less than 50,000 GRT Not later than first safety equipment survey after 1 July 2004 But before 31 December 2004 (whichever occurs earlier);
- Ships other than Passenger and Tankers of 50,000 GRT and upwards Not later than 1 July 2004;
- All new construction on or after 1 July 2004

8.2.2: If an AIS has not been installed on the ship before the International Ship Security Plan verification has been completed and it is not required to be installed until after 1 July 2004, the International Ship Security Certificate will be issued and remark will state the fact that the AIS has not been installed and the date the installation is required as defined in 8.2.1 above.

8.3 Continuous Synopsis Record (CSR):

(SOLAS Chapter XI-1 Regulation 5) All vessels are required to maintain a Continuous Synopsis Record, which includes a history of ownership and management of the ship. The Administration will provide all operators of Commonwealth of Dominica Ships with a form that lists the information on record regarding every ship in the Commonwealth of Dominica fleet. The Administration will maintain the record for Commonwealth of Dominica ships as long as they remain in the registry. The vessel operator is responsible for keeping the Administration informed of any changes regarding this record. Failure to keep the Administration informed is cause for removing the International Ship Security Certificate.

8.4 Ship's Security Alert:

(SOLAS Chapter X1-2 Regulation 6) All ships shall have a ship's security alert system installed to the satisfaction of the vessel's classification society by:

Type of vessel Constructed Compliance date:

- All ships constructed on or after 1 July 2004 on or after 1 July 2004;
- The following High-speed craft of 500 gross tonnage and upwards;
- Passenger Ships, Oil tankers, Chemical tankers, Gas carriers, Bulk carriers, Cargo Before 1 July 2004 Not later than first survey of radio the installation after 1 July 2004;
- Other cargo ships of 500 gross tonnage and upwards and Mobile offshore drilling units Before 1 July 2004 Not later than first survey of radio the installation after 1 July 2006

8.4.1: If the ship has not installed a Ship's Security Alert System on or before the International Ship Security Plan verification has been completed and it is not required to be installed until after 1 July 2004, the International Ship Security Certificate will be issued and remark will state the fact that the equipment has not been installed and the date the installation is required as defined in 8.4 above.

9. ADMINISTRATION'S PROGRAM FOR SETTING SECURITY LEVELS:**9.1 Guidance:**

The Administration has developed a program for setting security levels and is working on a system to provide guidance and security alerts to all CSO's through Email, fax, and direct contact to the vessels as appropriate. Higher security levels will indicate greater likelihood of occurrence of a security incident. The Administration will consider the following when setting the appropriate security level:

- The degree that the threat information is credible;
- The degree that the threat information is corroborated;
- The degree that the threat information is specific or imminent; and
- The potential consequences of such a security incident.
- The relevancy of the information to the vessel's operating area.

9.2 Instructions:

When setting levels 2 or 3, the Administration shall provide appropriate instructions and shall provide related information to specific ships, companies and other Contracting Governments as appropriate.

ANNEX I

Recognized Organizations authorized to conduct ISPS Code verification assessments and issue Certificates on behalf of the Commonwealth of Dominica:

ORGANIZATION ADDRESS CONTACT TEL/FAX

AMERICAN BUREAU OF SHIPPING
(ABS) ABS SESC Office Dubai
C/O ABS Dubai
Operations Ofc

ABS Pacific
438 Alexandra Road
#10-00, Alexandra Point
Singapore 119958

ABS Americas
16855 Northchase Drive
Houston, TX 77060
Captain Steve Blair
Ms Samantha Mulligan
Mr. Ravinder N. Chadha
Capt. Patrick L. Fallwell, Mgr.
Safety & Environmental Systems Certification
Tel: 971 4 352 0371
Fax: 971 4 355 5358
Email: sblair@eagle.org ; smulligan@eagle.org
Tel: 65.276.8700
Fax: 65.276.3880
Tlx: 34264 RS
Tel: 281.877.6057
Fax: 281.877.5932
Cell 281.731.3212
EMAIL: pfallwell@eagle.org

Northeast Maritime Institute
International Ship and Port Security Division
32 Washington Street
Fairhaven, Massachusetts 02719
Captain Frank Whipple
Tel: 508.992.4025
Fax: 508.992.9184
e-mail: fwhipple@northeastmaritime.com

- end -

18 of 18

Inquiries concerning the subject of this Circular should be directed to the Deputy Maritime Administrator
Commonwealth of Dominica 32 Washington Street, Fairhaven, MA 02719 USA
registration@dominica-registry.com