Commonwealth of Dominica

Office of the Maritime Administrator

TO: **ALL SHIPOWNERS, OPERATORS OF MERCHANT SHIPS, MOBILE OFFSHORE DRILLING UNITS AND AUTHORIZED CLASSIFICATION SOCIETIES**

SUBJECT: **GUIDANCE FOR DEVELOPING SHIP SECURITY PLANS**

REFERENCE: **(a) SOLAS, Chapter XI-2**
(b) ISPS Code

ATTACHMENTS: **Aid for reviewing compliance for Ship Security Plans**

PURPOSE: **The purpose of this Safety Circular is to provide guidance to all the owners and operators of the Commonwealth of Dominica flag vessels for developing Ship Security Plans.**

APPLICABILITY: **Dominica flag vessels engaged on international voyages, as follows:**
a) passenger vessels, including high-speed passenger craft;
b) cargo vessels, including high-speed craft, of 500 gross tonnage and upwards; and
c) mobile offshore drilling units.

PROVISIONS:

1 Dominica Maritime Administration has developed a tool for reviewing Ship Security Plans submitted for approval. Owners and Operators of Dominica flag vessels are advised to use the tool as guidance towards compliance with the provisions of SOLAS Chapter XI-2 and ISPS Code.

2 The tool: *Aid for reviewing compliance for Ship Security Plans* is attached as Annex to this Safety Circular.

- end -

Attachment: (1) Aid for reviewing compliance for Ship Security Plans

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

ANNEX

Aid for reviewing compliance for Ships Security Plans

The Ship Security Plan (SSP) should address the items noted to the degree appropriate to the ship. A copy of a general arrangement depicting restricted areas and access points should be included.

COMPLIANCE	YES (X)	NO (X)
Master		
1) Authority of Master to make decision to maintain the safety and security of the vessel.		
2) If there is a conflict between safety and security, Master can take action to best maintain the safety of the vessel. In such cases:		
a) The Master must notify the PFSO and DMRI;		
b) Security measures must be commensurate with the prevailing Security Level;		
c) Owner/operator must ensure that conflicts are resolved to the satisfaction of the DMRI for vessels on international voyages, and that recurrence is minimized.		
Company Security Officer (CSO)		
1) General.		
a) Owner/Operator must designate a CSO in writing.		
b) The CSO may delegate duties, but the CSO remains responsible for the performance of those duties.		
2) Qualifications.		
CSO must have general knowledge through training or equivalent experience in the following:		
a) Security administration and organization of company's vessels;		
b) Vessel, facility and port operations relevant to that industry;		
c) Vessel and facility security measures, requirements at the different Security Levels;		
d) Emergency preparedness and response and contingency planning;		
e) Security equipment and systems;		
f) Methods of conducting audits, and techniques for inspecting, controlling, and monitoring techniques;		
g) Techniques for security training and education, including security measures/procedures;		
h) Handling sensitive security-related information and security-related communications; **and**		
i) Knowledge of current security threats and patterns.		
3) Responsibilities		
In addition to duties specified elsewhere, the CSO for each vessel must:		
a) Keep vessel apprised of potential threats;		
b) Ensure a Ship Security Assessment is carried out;		
c) Ensure a Ship Security Plan (SSP) is developed, approved and implemented;		
d) Ensure the SSP is modified when necessary;		
e) Ensure the vessel's security activities are audited;		
f) Arrange for Administration or RO's verifications;		
g) Ensure timely correction of problems identified by audits;		
h) Enhance awareness and vigilance within the ship-owners organization;		
i) Ensure personnel receive adequate security training;		
j) Ensure communication/cooperation between SSO and relevant PFSOs;		
k) Ensure consistency between security requirements and safety requirements;		

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

l) Ensure that vessel specific information is included when several similar types vessel plans are submitted; **and**		
m) Ensure implementation and maintaining of alternative or equivalent arrangements, if approved.		
Ship Security Officer (SSO)		
1) General		
a) For manned vessels the SSO must be the Master or a member of the crew.		
b) For unmanned vessels the SSO must be a company employee and may serve as SSO for more than one unmanned vessel. If serving as SSO for more than one unmanned vessel, list of vessels for which responsible must be in the SSP.		
c) The SSO of any unmanned barge and the SSO of any interfacing towing vessel must coordinate/implement security measures for interfacing period.		
d) SSP may assign security duties to other vessel personnel; however SSO responsible.		
2) Qualifications		
SSO must have knowledge through training or equivalent job experience in the following:		
a) Security administration and organization of company's vessels;		
b) Vessel, facility and port operations relevant to that industry;		
c) Vessel and facility security measures, requirements at the different Security Levels;		
d) Emergency preparedness and response and contingency planning;		
e) Security equipment and systems and their operational limitations;		
f) Methods of conducting audits, and techniques for inspecting, controlling, and monitoring techniques;		
g) Techniques for security training and education, including security measures/procedures;		
h) Handling sensitive security-related information and security-related communications;		
i) Knowledge of current security threats and patterns;		
j) Ship layout;		
k) The SSP and related procedures including scenario-based response training;		
l) Crowd management and control techniques;		
m) Operation of security equipment and systems; **and**		
n) Testing, calibration, and at-sea maintenance of security equipment and systems.		
3) Responsibilities		
In addition to the duties and responsibilities mentioned elsewhere, the SSO must perform the following:		
a) Regularly inspect the vessel to ensure security measures are maintained;		
b) Ensure maintenance and supervision of implementation of the SSP and amendments;		
c) Coordinate handling of cargo and ship's stores with relevant PFSOs;		
d) Periodically review SSP and propose modifications of same to the CSO;		
e) Ensure any problems during audits/inspections are reported to the CSO and implement corrective actions;		
f) Ensure and enhance security awareness and vigilance onboard the vessel;		
g) Ensure adequate training for the vessel personnel;		
h) Ensure the reporting and recording of all security incidents;		
i) Ensure the coordination/implementation of the SSP with the CSO and relevant PFSO;		
j) Ensure security equipment is properly operated, tested, calibrated and maintained;		
k) Ensure consistency between security requirements and proper treatment of crew; **and**		
l) Acknowledge receipt of the instructions on change of the security level, whenever security level 2 or 3 is set by DMRI.		

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

Company Personnel with Security Duties		
These persons must have knowledge, through training or equivalent experience in the following areas:		
1) Vessel, facility and port operations relevant to that industry;		
2) Vessel and facility security measures, requirements at the different Security Levels;		
3) Emergency preparedness and response;		
4) Security equipment and systems;		
5) Handling sensitive security-related information and security-related communications;		
6) Knowledge of current security threats and patterns.		
7) Recognition of characteristics/behavioral patterns of those likely to threaten security;		
8) The meaning and consequential requirements of different Security Levels; **and**		
9) Relevant provisions of the security plan.		
Ship Personnel with Security Duties		
1) Qualifications.		
These persons must have knowledge, through training or equivalent experience in the following areas:		
a) Knowledge of current security threats and patterns;		
b) Recognition and detection of weapons, dangerous substances and devices;		
c) Recognition of characteristics/behavioral patterns of those likely to threaten security;		
d) Techniques used to circumvent security measures;		
e) Crowd management and control techniques;		
f) Security-related communications;		
g) Knowledge of emergency procedures and contingency plans;		
h) Operation of security equipment and systems;		
i) Testing, calibration and maintenance of security systems while at sea;		
j) Inspection, control and monitoring techniques;		
k) Methods of physical screening of persons, personal effects, baggage, cargo and vessels stores;		
l) Relevant provisions of the security plan; **and**		
m) The meaning and consequential requirements of different Security Levels.		
2) Responsibilities		
SSP must specify duties of shipboard personnel assigned security responsibilities on security aspects, at each Security Level.		
All Other Vessel Personnel		
1) Training		
All other personnel including contractors must have knowledge of, through training, or equivalent job experience in the following, as appropriate:		
a) Relevant provisions of the SSP;		
b) The consequential requirements of the different Security Levels;		
c) Knowledge of emergency procedures and contingency plans;		
d) Recognition and detection of weapons, dangerous substances and devices;		
e) Recognition and characteristics/behavioral patterns of those likely to threaten security; **and**		
f) Techniques used to circumvent security measures.		
2) Responsibilities		
SSP must specify duties of all other shipboard personnel on security aspects, at each Security Level.		

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

Drill and Exercise Requirements		
1) General		
a) Drills and exercises test the proficiency of the crew at different Security Levels and implement SSP. They must enable SSO to identify any related security deficiencies needed to be addressed.		
b) A drill or exercise may be satisfied with implementation of security measures required by SSP as result of increase in Security Level.		
2) Drills		
a) SSO must ensure that at least one security drill is conducted at least once every 3 months.		
b) Drills must test individual elements of the SSP including response to threats/incidents.		
c) If the vessel is at a facility, which is scheduled for a drill, the vessel may participate in same drill.		
d) Drill must be conducted within one week from when crew w/o drill experience on that vessel exceeds 25%.		
3) Exercises		
a) Exercises must be conducted each calendar year with no more than 18 months between exercises.		
b) Exercises may be:		
I) Full scale or live;		
II) Tabletop simulation or seminar;		
III) Combined with other appropriate exercises; **or**		
IV) A combination of elements in paragraphs (3) (b) (I) through (III) of this section.		
c) Exercises may be vessel specific or cooperative to incorporate facility/vessel/port exercises.		
d) Each exercise must test communication/notification/coordination/resources & response.		
Vessel Recordkeeping Requirements		
1) The SSO must keep records of activities in paragraph (2) of this section for at least 2 years.		
2) Records required by this section may be kept in electronic format and must be protected from unauthorized deletion, destruction or amendment. The following records must be kept:		
a) Training;		
b) Drills and exercises;		
c) Incidents and breaches of security;		
d) Changes in security levels;		
e) Communications relating to the direct security of the ship as specific threats to the ship or to port facilities the ship is, or has been, in;		
f) Internal audits and reviews of security activities;		
g) Periodic review of the ship security assessment and plan		
h) Implementation of any amendments to the plan;		
i) Maintenance, calibration and testing of security equipment, including testing of the ship security alert system;		
j) Security threats; **and**		
k) Declaration(s) of security.		
3) Any records required by this part must be protected from unauthorized access or disclosure.		
4) Records must be kept in the working language(s) of the ship and include translation into English, French or Spanish.		

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

Security Level Coordination and Implementation		
1) Owner/Operator must ensure prior to entering port or visiting an OCS facility, all measures taken as in SSP for compliance with Security Level in effect in that port/facility.		
2) When notified of increase in Security Level, vessel Owner/Operator must ensure the following:		
a) If higher Security Level set for port facility which vessel is in or about to enter, vessel complies without undue delay with all measures specified in SSP for compliance with that higher Security Level; **and**		
b) The respective PFSO is notified when compliance with higher Security Level is implemented.		
3) For **Security Level 1**, SSO must brief crew on possible threats, the procedures for reporting suspicious persons, objects or activities and need for vigilance		
4) For **Security Levels 2 and 3**, SSO must provide additional security briefings to crew on identified threats/reporting procedures, and stress need for high vigilance		
5) For **Security Level 3**, ship has to comply with the instructions issued by those responding to the security incident or threat thereof, including close co-operation with those responding and the port facility in undertaking security measures. Owner/Operator must ensure procedures for responding to any security instructions Contracting Governments may give.		
6) For **Security Level 3**, Owner/Operator may be required to implement additional measures that may include the following:		
a) Arrangements to ensure that vessel can be towed or moved if deemed necessary by respective PFSO;		
b) Use of waterborne security patrol with co-operation of port facility; **or**		
c) Screening the vessel for presence of dangerous substances and devices underwater or other threats, with co-operation of port facility.		
Communications		
1) The SSO must have a means to effectively notify crew of changes in security conditions onboard vessel.		
2) Communication systems and procedures must allow effective and continuous communication between ship security personnel, interfacing facilities/vessels and national or local authorities with security responsibilities.		
3) Communication systems and procedures must enable vessel personnel to notify shore side authorities or other vessels of a security threat or incident onboard in a timely manner.		
Procedures for Interfacing with Facilities and Other Vessels		
Vessel Owner/Operator must ensure interface measures with other vessels/facilities at all Security Levels.		
Declaration of Security (DOS)		
1) Each vessel must have procedures for requesting DoS and handling DoS requests from facility or other vessel.		
2) The DoS should be completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships, as applicable.		
3) DoS shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.		

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

4) At **Security Level 2**, for cruise ship or manned vessel with dangerous cargo in bulk, respective Master/SSO/designee before vessel-to-vessel/facility interface and prior to passenger/cargo transfer must sign DoS with respective Master/SSO/PFSO/designee.		
5) At **Security Level 3**, respective Master/SSO before vessel-to-vessel/facility interface and prior to passenger/cargo transfer must sign DoS with respective Master/SSO/PFSO.		
Security Systems and Equipment Maintenance		
1) Security systems/equipment to be in good order and tested, calibrated and maintained according to manufacturer's recommendations.		
2) Results of tests as per paragraph (1) to be recorded in accord with relevant provisions. Deficiencies to be promptly corrected.		
3) SSP must include procedures for identifying and responding to security equipment failures/malfunctions.		
Security Measures for Access Control		
1) General		
Vessel Owner/Operator must ensure implementation of security measures to:		
a) Prevent unauthorized introduction of weapons, dangerous substances or devices;		
b) Secure dangerous substances that are authorized by the owner to be onboard; **and**		
c) Control access to the vessel;		
2) The vessel owner or operator must ensure the following are specified:		
a) Access locations where restrictions are applied for each Security Level. Means of access include but are not limited to the following:		
I) Access ladders;		
II) Access gangways;		
III) Access ramps;		
IV) Access doors, side scuttles, windows and ports;		
V) Mooring lines and anchor chains; **and**		
VI) Cranes and hoisting gear.		
b) Types of restrictions to be applied and the means of enforcing them at each location, for each security level,; **and**		
c) The means of identification required to allow persons to access the vessel and remain onboard without challenge, for each security level.		
3) Owner/Operator to ensure ID system to check crew/others seeking access to the vessel that:		
a) Allows ID of authorized and unauthorized persons at any Security Level;		
b) Is coordinated with ID system at facilities used by the vessel when practical;		
c) Is updated regularly;		
d) Uses disciplinary measures to discourage abuse; **and**		
e) Allows temporary or continuing access for crew and visitors through use of badge or other system.		
4) The Owner/Operator must include in SSP frequency of application of security measures for access control.		
5) Security Level 1		
Owner/Operator must ensure that the security measures in this paragraph are implemented to:		
a) Conspicuously post signs describing security measures in effect and clearly stating:		
I) Boarding the vessel is deemed valid consent to screening or inspections; **and**		
II) Failure to consent to screening/inspection will result in denial or revocation of authorization to board.		

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

b) Check ID of any person seeking to board the vessel, including vendors, passengers, crew, visitors, etc. This check includes confirming the reason for boarding by examining at least one of the following:		
I) Joining instructions;		
II) Passenger tickets;		
III) Boarding passes;		
IV) Work orders, pilot orders, or survey orders;		
V) Government identification; **or**		
VI) Visitor badges issued in accordance with an ID system required in paragraph (3) of this section;		
c) Deny or revoke a person's authorization to be onboard if unable or unwilling to establish ID. Any such incident must be reported in compliance with this part;		
d) Deny unauthorized access to the vessel;		
e) Identify access that must be secured or attended to deter unauthorized access;		
f) Lock or prevent access to unattended spaces that adjoin areas to which passengers/visitors have access;		
g) In liaison with the port facility ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry-on items), personal effects, vehicles and their contents can take place;		
h) Crew is not required to engage in inspection/screening of other crewmembers;		
i) Ensure checked persons and their personal effects are segregated from unchecked persons;		
j) Ensure embarking passengers are segregated from disembarking passengers; **and**		
k) Ensure a defined percentage of vehicles to be loaded on board car carriers, ro-ro and other passenger vessels are searched before loading at the rate indicated in the SSP.		
6) Security Level 2		
The additional security measures required may include the following:		
a) Increasing the frequency and detail of screening people, personal effects and vehicles being embarked;		
b) Assigning additional personnel to patrol decks during periods of reduced vessel operations;		
c) Limiting the number of access points to the vessel by closing and securing some;		
d) Escorting visitors on the ship;		
e) Deterring waterside access to the vessel which may include the facility providing boat patrols; **and**		
f) Establishing a restricted area on the shore side of the vessel in cooperation with the facility.		
7) Security Level 3		
The additional security measures required may include the following:		
a) Screening all persons, baggage and personal effects for dangerous substances and devices;		
b) Being prepared to cooperate with responders and facilities;		
c) Limiting access to the vessel to a single controlled access point;		
d) Granting access to only those responding to the security incident or threat;		
e) Suspending embarkation or disembarkation;		
f) Suspending cargo operations, deliveries, etc.;		
g) Evacuating the vessel;		
h) Moving the vessel; **and**		
i) Preparing for a full or partial search of the vessel.		

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

Security Measures for Restricted Areas		
1) General		
The Owner/Operator must ensure the designation of restricted areas in order to:		
a) Prevent or deter unauthorized access;		
b) Protect persons authorized to be onboard;		
c) Protect security-sensitive areas within the vessel;		
d) Protect security and surveillance equipment and systems; **and**		
e) Protect cargo and vessel stores from tampering.		
2) Designation of restricted areas		
Owner/Operator must ensure restricted areas are designated as specified in the approved SSP. Restricted areas must include, as appropriate:		
a) Navigation bridge, machinery spaces, and other control spaces;		
b) Spaces containing security and surveillance equipment, and their controls and lighting system controls;		
c) Ventilation and A/C systems, and other similar spaces;		
d) Spaces with access to portable water tanks, pumps or manifolds;		
e) Spaces containing dangerous goods or hazardous substances;		
f) Spaces containing cargo pumps and their controls;		
g) Cargo spaces and spaces containing vessels stores;		
h) Crew accommodations; **and**		
i) Any other spaces or areas vital to the security of the vessel.		
3) Owner/Operator must ensure that security measures and policies are established to:		
a) Identify which vessel personnel are authorized to have access;		
b) Determine which persons other than vessel personnel are authorized to have access;		
c) Determine the conditions under which that access may take place;		
d) Define the extent of any restricted area;		
e) Define the times when access restrictions apply; **and**		
f) Clearly mark all restricted areas and that unauthorized presence constitutes a breach of security.		
4) Security Level 1		
Owner/Operator must ensure security measures to prevent unauthorized access. Security measures may include:		
a) Locking or securing access points;		
b) Monitoring or using surveillance equipment;		
c) Using guards or patrols; **and**		
d) Using automatic intrusion-detection devices to activate audible/visual alarm at a location continuously attended or monitored to alert vessel personnel of unauthorized access.		
5) Security Level 2		
In addition to measures taken at Level 1, additional measures may include the following:		
a) Increasing the frequency and intensity of monitoring and access controls on existing restricted access areas;		
b) Restricting access to areas adjacent to access points;		
c) Continuously monitoring surveillance equipment; **and**		
d) Dedicating additional personnel to guard or patrol each area.		
6) Security Level 3		
In addition to measures taken at Levels 1 and 2, additional measures may include the following:		
a) Denying access to additional areas in proximity to the security incident or the believed location of the security threat; **and**		
b) Searching restricted areas as part of a security sweep of the vessel.		

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

Security Measures for Handling Cargo		
1) General		
Owner/Operator must ensure security measures related to cargo handling are specified in order to:		
a) Deter tampering;		
b) Prevent cargo not meant for carriage from being accepted and stored on the vessel;		
c) Identify cargo that is approved for loading onto the vessel;		
d) Include inventory control procedures at access points to the vessel; **and**		
e) When there are regular/repeated cargo ops with same shipper, coordinate security measures with the shipper/responsible party in accordance with established agreement and procedures. Such arrangements should be communicated to and agreed with the PFSO concerned.		
2) Security Level 1		
Owner/Operator must ensure the implementation of measures to:		
a) Unless unsafe to do so; routinely check cargo and cargo spaces prior to and during cargo handling for evidence of tampering;		
b) Check that cargo to be loaded matches the cargo documentation or container numbers match shipping documents;		
c) Ensure in liaison with facility, that vehicles loaded on RO-RO and passenger ships are screened before loading as per frequency specified in SSP; **and**		
d) Check in liaison with facility, seals or other methods used to prevent tampering.		
3) Security Level 2		
Owner/Operator to ensure implementation of additional security measures which may include the following:		
a) Increase the frequency and detail of checking cargo and cargo spaces for evidence of tampering;		
b) Intensify checks to ensure that only intended cargo is loaded;		
c) Intensify screening of vehicles to be loaded on car carriers, RO-RO and passenger vessels;		
d) In liaison with facility, increasing frequency and detail in checking seals and other methods used to prevent tampering; **and**		
e) Increasing frequency and intensity of visual and physical inspections; **or**		
f) Coordinating enhanced security measures with the shipper or other party i/a/w established agreement and procedures.		
4) SECURITY Level 3		
In addition to measures at Level 1 and 2, additional measures which may include:		
a) Suspending loading or unloading of cargo;		
b) Being prepared to cooperate with responders, facilities, and other vessels; **and**		
c) Verifying the inventory and location of any hazardous materials carried on board.		
Security Measures for Delivery of Vessel Stores and Bunkers		
1) General		
Owner/Operator must ensure security measures for delivery of stores/bunkers are implemented to:		
a) Check vessel stores for package integrity;		
b) Prevent vessel stores from being accepted without inspection;		
c) Deter tampering; **and**		
d) Prevent vessel stores and bunkers from being accepted unless ordered.		

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

2) SECURITY Level 1		
Owner/Operator must ensure the implementation of measures to:		
a) Check that stores or bunkers match the order prior to being brought onboard or bunkered; **and**		
b) Ensure stores are controlled or immediately and securely stowed following delivery.		
3) SECURITY Level 2		
In addition to measures taken at Level 1, additional security measures may include:		
a) Intensify the inspection of vessel stores during delivery; **or**		
b) Checking vessel stores prior to receiving them onboard.		
4) SECURITY Level 3		
In addition to security measures at Levels 1and 2, additional security measures may include:		
a) Checking all vessel stores more extensively;		
b) Restricting or suspending delivery of vessel stores and bunkers; **or**		
c) Refusing to accept vessel stores onboard.		
Security Measures for Handling Unaccompanied Baggage		
1) General		
Owner/Operator must ensure the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search), before it is accepted on board the ship, is:		
a) Identified; **and**		
b) Subjected to appropriate screening, including searching.		
2) SECURITY Level 1		
Owner/Operator must ensure the implementation of measures to ensure the screening or searching of up to 100% of unaccompanied baggage		
3) SECURITY Level 2		
Owner/Operator must ensure the implementation of additional security measures to ensure X-ray screening of all unaccompanied baggage.		
4) SECURITY Level 3		
In addition to security measures at Levels 1and 2, additional security measures may include:		
a) Screen unaccompanied baggage more aggressively, for example, X-ray from two or more angles;		
b) Prepare to restrict or suspend handling unaccompanied baggage; **and**		
c) Refuse to accept unaccompanied baggage onboard;		
Security Measures for Monitoring		
1) General		
a) Owner/Operator to ensure the implementation of security measures by continuously monitoring through a combination of lighting, watch keepers, security guards, deck watches, waterborne patrols, auto intrusion-detection devices, or surveillance equipment of the following:		
I) Vessel;		
II) Restricted areas onboard the vessel; **and**		
III) Areas surrounding the vessel.		
b) The following must be considered when establishing the appropriate level & location of lighting:		
I) Vessel personnel should be able to detect activities on & around vessel on both shore side& waterside;		
II) Coverage should facilitate personnel identification at access points;		

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

III) Coverage may be provided through coordination with the port or facility; **and**		
IV) Lighting effects (such as glare) and its impact on safety, navigation, and other security activities.		
2) SECURITY Level 1		
Owner/Operator to ensure security measures that may be done in coordination with facility to:		
a) Monitor the vessel, particularly vessel access points and restricted areas;		
b) Ensure that equipment or system failures or malfunctions are identified and corrected;		
c) Ensure that automatic intrusion detection device sets off audible/visual alarm at location continuously attended or monitored;		
d) Illuminate deck and access points from sunset to sunrise and during periods of low visibility to enable ID of persons seeking access to vessel; **and**		
e) Use maximum available lighting underway from sunset to sunrise consistent with safety and international regs.		
3) SECURITY Level 2		
In addition to security measures at Level 1, additional security measures may include:		
a) Be able to conduct emergency searches of the vessel;		
b) Increasing the frequency and details of security patrols;		
c) Increasing the intensity and coverage of lighting, alone or in conjunction with facility;		
d) Using or increasing the use of security/surveillance equipment.		
e) Assigning additional personnel as security lookouts;		
f) Coordinating with boat patrols when provided; **or**		
g) Coordinating with shore-side foot or vehicle patrols; when provided.		
4) SECURITY Level 3		
In addition to security measures at Levels 1 and 2, additional security measures may include the following:		
a) Switching on all lights;		
b) Illuminating the vicinity of the vessel;		
c) Activating all on-board surveillance equipment capable of recording activities on or in vicinity of the vessel;		
d) Maximizing the length of time such surveillance equipment can continue to record;		
e) Preparing for underwater inspection of the hull; **and**		
f) Initiating measures, including slow revolution of propeller(s), to deter underwater access to the vessel hull.		
Security Incident Procedures		
For **each SECURITY Level,** the Owner/Operator must ensure (provide procedures) the SSO & ship security personnel are able to:		
1) Respond to security threats or breaches of security and maintain critical vessel and vessel-to- facility operations to include:		
a) To prohibit entry into affected area;		
b) Deny access to the vessel except to those responding to the emergency;		
c) Implement SECURITY Level 3 security measures throughout the vessel;		
d) Stopping cargo handling operations; **and**		
e) Notify shore side authorities or other vessels of the emergency;		
f) Evacuate the vessel in case of security threats or breaches of security;		
g) Report security incidents;		
h) Brief all vessel personnel on possible threats and the need for vigilance as well as soliciting their assistance; **and**		
i) Secure non-critical operations in order to focus response on critical operations.		

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

Additional Requirements - Passenger Vessels and Ferries		
1) At **all SECURITY Levels**, the Owner/Operator must ensure that security sweeps are performed prior to getting underway and after any period the vessel was unattended.		
2) As an alternative to ID checks and passenger requirements, the Owner/Operator may ensure security measures are implemented that include:		
a) Searching selected areas prior to embarking passengers and prior to sailing; **and**		
b) Implementing one or more of the following:		
I) Performing routine security patrols;		
II) Providing additional closed circuit TV's to monitor passenger areas; **or**		
III) Securing all non-passenger areas.		
3) Masters/SSOs of passenger vessels that use public access facilities must sign DoS with respective Security Officers of public access facilities.		
4) At SECURITY Levels 2 and 3, in addition to Level 1 measures, Owner/ Operator must, as an alternative to the ID and screening requirements, intensify patrols, security sweeps and monitoring identified in paragraph b) of this section.		
Additional Requirements - Cruise Ships		
1) At all SECURITY Levels the Owner/Operator must ensure measures to:		
a) Screen all persons, baggage and personal effects for dangerous substances and devices;		
b) Check the ID of all persons seeking to board the vessel; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, govt ID etc;		
c) Perform security patrols; **and**		
d) Search selected areas prior to embarking passengers and prior to sailing.		
2) At SECURITY Level 3, the Owner/Operator must ensure that security briefs are given to passengers about the specific threat.		
Additional Requirements - Vessels on International Voyages		
1) An Owner/Operator of a Dominica flag vessel subject to SOLAS, 1974, must be in compliance with the applicable requirements of SOLAS Chapter XI-1, SOLAS Chapter XI-2, ISPS Code, Part A and the respective Commonwealth of Dominica Marine Safety Circulars.		
2) Owners/Operators of Dominica flagged vessels that are required to comply with SOLAS must ensure an ISSC is obtained for the vessels. This Certificate must be issued by DMRI and carried on vessel.		
Ship Security Assessment (SSA)		
Ship Security Assessment (SSA) requirements		
1) SSA report.		
a) Vessel Owner/Operator must ensure that a written SSA report is prepared and included as part of the SSP. The SSA report must contain:		
I) A summary of how the on-scene survey was conducted;		
II) Existing security measures, procedures and operations;		
III) A description of each vulnerability found during the assessment;		
IV) A description of security countermeasures that could be used to address each vulnerability;		
V) A list of the key shipboard operations that are important to protect;		
VI) The likelihood of threats to key vessel operations; **and**		
VII) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.		

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

b) The SSA report must address the following elements onboard or within the vessel:		
I) Physical security;		
II) Structural integrity;		
III) Personnel protection systems;		
IV) Procedural policies;		
V) Radio and telecommunication systems, including computer systems and networks **and;**		
VI) The other areas that may, if damaged or used illicitly, pose a risk to people, property or operations on board the vessel or within a facility.		
c) The SSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:		
I) Vessel personnel;		
II) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;		
III) Capacity to maintain safe navigation and emergency response;		
IV) Cargo, particularly dangerous goods and hazardous substances;		
V) Vessel stores;		
VI) Any vessel security communication and surveillance systems; **and**		
VII) Any other vessel security systems, if any;		
d) The SSA report must account for any vulnerabilities in the following areas;		
I) Conflicts between safety and security measures;		
II) Conflicts between vessel duties and security assignments;		
III) The impact of watch keeping duties and risk of fatigue on vessel personnel alertness and performance;		
IV) Security training deficiencies; **and**		
V) Security equipment and systems, including communication systems.		
e) The SSA report must discuss and evaluate key vessel measures and operations, including:		
I) Ensuring performance of all security duties;		
II) Controlling access to the vessel, through the use of identification systems or otherwise;		
III) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);		
IV) Supervising the handling of cargo and the delivery of vessel stores;		
V) Monitoring restricted areas to ensure that only authorized persons have access;		
VI) Monitoring deck areas and areas surrounding the vessel; **and**		
VII) The ready availability of security communications, information, and equipment.		
5) The SSA must be documented and the SSA report retained by the vessel owner or operator with the SSP. The SSA, the SSA report and SSP must be protected from unauthorized access or disclosure.		
SOLAS Chap XI-2/6 Ship Security Alert System (SSAS)		
1) Owner/Operator of the vessel shall provide the ship with an SSAS as per schedule in reg. XI-2/6.1. The system, when activated, shall:		
a) Initiate and transmit ship-to-shore alert to a competent Authority;		
b) Not send the ship security alert to other ships;		
c) Not raise any alarm on board the ship; **and**		
d) Continue the ship security alert until deactivated and/or reset.		
2) The SSAS shall:		
a) Be capable of being activated from the navigation bridge and at least one other location; **and**		
b) Conform to performance standards not inferior to those adopted by IMO.		

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

3) The SSAS activation points shall be designed so as to prevent inadvertent initiation.		
4) Equivalent SSAS compliance is radio installation meeting all standards of Chap IV.		
Administrative:		
Enter the following information		
Company address		
CSO designated + 24 hour contact details		
SSO named		
IMO Number		
Ship name and particulars with a copy of a general arrangement depicting restricted areas and access points.		

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