## Introduction

1. This Guidance applies to shipping companies and their employed on Myanmar flagged ships.

2. The purpose of this Guidance is to enhance maritime security and through which ships and port facilities can operate to detect and deter acts which threaten security in the maritime transport sector.

3. The Administration directs that measures are established by shipping companies and ship masters in accordance with the relevant International Convention for the Safety of Life at Sea 1974, as amended and Guide to Maritime security and the ISPS Code**,** as amended.

4. This National Guidance for Special Measures to enhance Maritime Security is set out on 6th October 2017 according to the Notification 8/2017 in the exercise of the power of Section 294 (B), paragraph (b) of Myanmar Merchant Shipping Act 1923, as amended.

# NATIONAL GUIDANCE FOR SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

## CONTENTS


| | | |
|---|---|---|
| 1. | Purpose | 4 |
| 2. | Application | 4 |
| 3. | Definitions | 4 |
| 4. | National Authorities and Recognized Security Organizations | 8 |
| 5. | Documentation | 11 |
| 6. | Audits | 12 |
| 7. | Security levels | 12 |
| 8. | Company Security Officer | 14 |
| 9. | Ship Security Officer | 16 |
| 10. | Documentation | 19 |
| 11. | Training, drills and exercises | 21 |
| 12. | Physical Security | 22 |
| 13. | Operational security | 24 |
| 14. | International Ship Security Certificate (ISSC) | 26 |
| 15. | Security Obligations | 34 |
| 16. | Incident response | 35 |
| 17. | Best management practices | 36 |
| 18. | Form of Certificates | 40 |

## 1. Purpose

The purpose of this Guidance is to promulgate all laws, decrees, orders and regulations necessary to give full and complete effect to chapter XI-2 of the Convention for the safety of Life at Sea, 1974, as amended (SOLAS),Guide to Maritime Security and the International Ship and Port facility Security (ISPS) Code.

## 2. Application

This Guidance shall be applied to the following Myanmar flagged ships engaged on international voyages;

.1 passenger ships, including high-speed passenger craft;

.2 cargo ship, includes high – speed craft , of 500 gross tonnage and upwards; and

.3 Mobile Offshore Drilling Units.

## 3. Definitions

**3.1 Administration** means the Government of the State whose flag the ship is entitled to fly. In the Maritime Security Measures and this Guide, "Administration" is used to describe the organization within Government responsible for ship security.

**3.2 Certification** means issuing International Ship Security Certificates (ISSCs), Interim ISSCs and Statements of Compliance for port facilities (optional).

**3.3 Clear grounds** means reasons for believing that a ship does not comply with requirements of the Maritime Security Measures.

**3.4 Company** means the owner of the ship or any other organization or person, such as the manager or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who, on assuming such responsibility, has agreed to take over all the duties and responsibilities imposed by the International Safety Management (ISM) Code.

**3.5 Company security officer (CSO)** means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained; and for liaison with port facility security officers and the ship security officer.

**3.6 Competent authority** means an organization designated by an Administration to receive and act on a ship-to-shore security alert.

**3.7 Compliance verifications** means undertaking intermediate and renewal verifications of compliance for ISSC issuance.

**3.8 Continuous Synopsis Record (CSR)** is a record maintained and updated throughout a ship's life and issued by the ship's Administration under SOLAS chapter XI-I, "Special measures to enhance maritime safety", containing information, including the name of the Administration or Contracting Government who issued the ship's current ISSC or Interim ISSC and the name of the body who carried out the verification of which the Certificate was issued if not the Administration or Contracting Government. The original names of those who issued previous International Ship Security Certificates have to remain in the CSR.

**3.9 Contracting Government** means a Government that has agreed to be bound by the SOLAS Convention. In this Guide the simpler term "Government" is generally used in place of "Contracting Government" unless there is a direct quotation from SOLAS chapter XI-2 or from the ISPS Code part A or part B. Depending on the context, "Government" can also be used in IMO Maritime Security Measures with either the term "Administration" or "Designated Authority", or with both, or in place of either or both.

**3.10 Control and compliance measures** mean actions that can be taken by a duly authorized officer when it is believed that clear grounds exist that a foreign-flagged ship does not comply with the requirements of the Maritime Security Measures; notifying the relevant Government when such measures *have* been applied to a ship, designating the contact point to receive communication from Governments exercising control and compliance measures, and communicating the contact details to IMO.

**3.11 Declaration of Security (DoS)** means an agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement.

**3.12 Deficiency** means a failure to comply with the requirements of the Maritime Security Measures.

**3.13 Designated Authority** means the Department of Marine Administration, as responsible for ensuring the implementation of the provisions of the Maritime Security Measures pertaining to port facility security and ship/port interface, from the point of *view* of the port facility. In the ILO/IMO Code of practice on security in ports the term is used to describe the organization within Government responsible for port security.

**3.14 Duly authorized officer** means a Government official given specific authorization to undertake official duties, usually associated with inspection and enforcement activities.

Such duties under the Maritime Security Measures include undertaking control and compliance measures in respect of foreign-flagged *vessels* under the Maritime Security Measures, and the use of the term in this Guide is usually associated with that activity.

**3.15 ILO/IMO Code of practice** means the ILO/IMO Code of practice on security in ports *Interim International Ship Security Certificate (Interim ISSC)* is a Certificate issued by, or on behalf of,

**3.16 International Safety Management (ISM) Cod** means the International Management Code for the Safe Operation of Ships and for Pollution Prevention required to be carried by all SOLAS ships under SOLAS chapter IX, "Management for the safe operation of ships".

**3.17 International Ship and Port Facility Security (ISPS) Code** means the International Code for the Security of Ships and of Port Facilities, consisting of part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory).

**3.18 International Ship Security Certificate (ISSC)** is a Certificate issued following verification by, or on behalf of, the ship's Administration that the ship complies with the requirements in SOLAS chapter XI-2 and the ISPS Code.

**3.19 International voyage** means a voyage from a country to which the SOLAS Convention applies to a port outside such a country, or conversely (SOLAS chapter I, "General provisions").

**3.20 Maritime Security Measures** means SOLAS chapter XI-2, "Special measures to enhance maritime security", and the ISPS Code, parts A and B.

**3.21 Port facility** means a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate.

**3.22 Port facility security officer (PFSO)** means the person designated as responsible for tile development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

**3.23 Port facility security plan (PFSP)** means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

**3.24 Port security officer (PSO)** means the person tasked to manage and co-ordinate security in the port.

**3.25 Port security plan (PSP)** means a plan developed to ensure the application of measures designed to protect the port and ships, persons, cargo, cargo transport units and ship's stores within the port from the risks of a security incident.

**3.26 Recognized security organization (RSO)** means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations that is authorized to carry out an assessment, or a verification, or an approval or a certification activity required by the Maritime Security Measures.

**3.27 Security incident** means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity.

**3.28 Security level** means the qualification of the degree of risk that a security incident will be attempted or will occur.

**3.29 Security level 1** means the *level* for which minimum appropriate protective security measures shall be maintained at all times.

**3.30 Security level 2** means the *level* for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

**3.31 Security level 3** means 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.

**3.32 Security plans:** approving security plans submitted by port facilities (PFSPs) and shipping companies (SSPs), and any subsequent amendments.

**3.33 Ship** means a passenger ship carrying more than 12 passengers or a cargo ship engaged in an international *voyage,* and includes high-speed craft and mobile offshore drilling units (MODUs). Generally, the provisions of the SOLAS *Convention* apply to cargo ships of, or *over,* 500 gross tonnage (GT). The Maritime Security Measures apply to passenger ships, as *above,* and to cargo ships *over* 500 GT. *However,* certain provisions from chapter V, *"Safety* of *navigation",* of the SOLAS Convention also specifically apply to cargo ships of, or *over,* 300 GT, including mandatory fitting of equipment associated with automatic identification systems (AIS) and long-range identification and tracking (LRLT) systems.

**3.34 Shipboard personnel** means the master and the members of the crew or other persons employed or engaged in any capacity on board a ship in the business of that ship, including high-speed craft, special-purpose ships and mobile offshore drilling units not on location.

**3.35 Ship/port interface** means the interactions that occur when a ship is directly and immediately affected by actions involving the *movement* of persons, goods or the provisions of port services to or from the ship.

**3.36 Ship security alert system (SSAS)***:* provides the means by which a ship can transmit a security alert to a competent authority on shore, indicating that the security of the ship is under threat or has been compromised.

**3.37 Ship security assessment** means a risk assessment undertaken by, or for, a company security officer as a prelude to the preparation of a ship security plan or the review, or amendment, of an approved ship security plan.

**3.38 Ship security officer (SS0)** means the person on board the ship, accountable to the master, who is 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 and port facility security officers.

**3.39 Ship security plan (SSP)** means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

**3.40 Ship-to-ship activity** means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

**3.41 Short international voyage** is an international voyage in the course of which a ship is not at any time more than 200 miles from a port or a place in which the passengers and crew could be placed in safety. Neither the distance between the last port of call in the country in which the voyage begins and the final port of destination, nor the return voyage, shall exceed 600 miles. The final port of destination is the last port of call in the scheduled voyage at which the ship commences its return voyage to the country in which the voyage began.

**3.42 SOLAS Convention** means the International Convention for the Safety of Life at Sea, 1974, as amended.

**3.43 Threat** is the likelihood that an unlawful act will-be committed against a particular target, based on a perpetrator's intent and capability.

## 4. National Authorities and Recognized Security Organizations

**4.1** Department of Marine Administration (DMA) is to regulate port facility security and ship security.

**4.1.1** Pursuant to SOLAS chapter XI-2 and part A of the ISPS Code, DMA is responsible for:

.1 setting the applicable security level;

.2 approving the Ship security plan and relevant amendments to a previously approved plan;

.3 verifying the compliance of ships with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code and issuing to ships the International Ship Security Certificate;

.4 determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port facility security plan;

.5 ensuring completion and approval of the Port facility security assessment and of any subsequent amendments to a previously approved assessment;

.6 approving the Port facility security plan and any subsequent amendments to a previously approved plan;

.7 exercising control and compliance measures;

.8 testing approved plans; and

.9 communicating information to the International Maritime Organization and to the shipping and port industries.

**4.2** DMA will delegate to a recognized security organization certain of security-related duties under SOLAS chapter XI-2 and part A of the ISPS Code.

**4.2.1** When authorizing a recognized security organization, DMA shall give consideration to the competency of such an organization. A recognized security organization should be able to demonstrate:

.1 expertise in relevant aspects of security;

.2 appropriate knowledge of ship operations, including knowledge of ship design and construction if providing services in respect of ships;

.3 capability to assess the likely security risks that could occur during ship operations including the ship/port interface and how to minimize such risks;

.4 ability to maintain and improve the expertise of their personnel;

.5 ability to monitor the continuing trustworthiness of their personnel;

.6 ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material;

.7 knowledge of the requirements of SOLAS chapter XI-2 and part A of the ISPS Code and relevant national and international legislation and security requirements;

.8 knowledge of current security threats and patterns;

.9 knowledge on recognition and detection of weapons, dangerous substances and devices;

.10 knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.11 knowledge on techniques used to circumvent security measures; and

.12 knowledge of security and surveillance equipment and systems and their operational limitations.

**4.2.2** When delegating specific duties to a recognized security organization, DMA shall ensure that the recognized security organization has the competencies needed to undertake the task.

**4.2.3.** DMA will authorize a recognized security organization to undertake certain security-related activities, including:

.1 approval of ship security plans, or amendments there to, on behalf of the Administration;

.2 verification and certification of compliance of ships with the requirements of SOLAS chapter XI-2 and part A of the ISPS Code on behalf of the Administration.

**4.2.4** A recognized security organization will also advise or provide assistance to companies on security matters, including ship security assessments, ship security plans. This can include completion of a ship security assessment or plan.

**4.2.5** DMA retain ultimate responsibility for the work undertaken on their behalf by the recognized security organizations that they appoint. They have the authority to modify or revoke their delegations to a recognized security organization which fails to meet agreed performance standards.

## 5 Documentation

### 5.1 Security assessments

**5.1.1** The ship security assessments are an essential and integral part of the process

of developing and updating the ship security plans, respectively.

## 5.2 Security plans

**5.2.1** The legislation shall set out the requirements and the procedures applying to:

.1 the submission of ship security plans;

.2 the approval of ship security plans, with or without modification;

.3 the requirements to review an approved ship security plan;

.4 the submission of amendments to an approved ship security plan; and

.5 consideration of any applications for exemptions from holding a plan, consistent with SOLAS regulation 1/4(a).

**5.2.2** DMA shall ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to ship security assessments, ship security plans and to individual assessments or plans.

### 5.2.3 Declarations of security

**5.2.3.1** DMA shall determine when a declaration of security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment.

**5.2.3.2** The declaration of security 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.

**5.2.3.3** A ship will request completion of a declaration of security when:

.1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;

.2 there is an agreement on a declaration of security between governments covering certain international voyages or specific ships on those voyages;

.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

.4 the ship is at a port which is not required to have and implement an approved port facility security plan; or

.5 the ship is conducting ship-to-ship activities with another ship not required to have and implement an approved ship security plan.

### 5.2.4 Records

**5.2.4.1** Ships shall keep records of the last 10 calls at port facilities.

**5.2.4.2** Records of the following activities shall be kept on board for the minimum period 3years specified by DMA

.1 training, drills and exercises;

.2 security threats and security incidents;

.3 breaches of security;

.4 changes in security level;

.5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been in;

.6 internal audits and reviews of security activities;

.7 periodic review of the ship security assessment;

.8 periodic review of the ship security plan;

.9 implementation of any amendments to the plan; and

.10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

**5.2.4.3** The records shall be protected from unauthorized access or disclosure.

## 6 Audits

**6.1** Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the company or of the ship.

## 7 Security levels

**7.1** The three levels of risk are now used internationally:

.1 "security level 1" means the level for which minimum appropriate protective security measures shall be implemented at all times.

.2 "security level 2" means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of the heightened risk of a security incident.

.3 "security level 3" means 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 a specific target.

## 7.2 Security level 1

**7.2.1** At security level 1, the following activities shall be carried out through appropriate measures in all ships and/or port facilities, taking into account the guidance given in part B of the ISPS Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship and/or port facility security duties;

.2 controlling access to the ship and/or port facility;

.3 controlling the embarkation of persons and their effects;

.4 monitoring of the ship deck and/or port facility, including anchoring and berthing area(s) and areas surrounding the ship;

.5 monitoring restricted areas to ensure that only authorized persons have access;

.6 supervising the handling of cargo and ship's stores; and

.7 ensuring that security communication is readily available.

## 7.3 Security level 2

**7.3.1** At security level 2, the additional protective measures, specified in the ship and/or port facility security plan, shall be implemented for each required activity, taking into account the guidance given in part B of the ISPS Code.

## 7.4 Security level 3

**7.4.1** At security level 3, further specific protective measures, specified in the ship and/or port facility security plan, shall be implemented for each required activity, taking into account the guidance given in part B of the ISPS Code.

## 7.5 Security level coordination

**7.5.1** Ships intending to enter a port or port facility should establish the applicable security level through direct contact with the port authority, or the Port Security Officer or the Port Facility Security Officer, prior to entry. If a ship is operating at a higher security level than that applying at the port or port facility, the information should be passed to the port authority or the Port Security Officer or the Port Facility Security Officer prior to entry.

**7.5.2** A ship can never operate at a lower security level than the one being applied at the port or port facility that it is visiting.

**7.5.3** A ship can, however, operate at a higher security level than that applying at the port or port facility it is in, or it intends to enter. The authorities at the port/port facility should not seek to have the ship reduce the security level set by the ship's government.

## 8. Company Security Officer

**8.1** The Company shall designate a Company Security Officer. A person designated as the Company Security Officer may act as the Company Security Officer for one or more ships, depending on the number or types of ships the company operates provided it is clearly identified for which ships this person is responsible. A company may, depending on the number or types of ships they operate designate several persons as Company Security Officers provided it is clearly identified for which ships each person is responsible.

**8.2** Every person designated as a Company Security Officer should be able to demonstrate competence to undertake the following tasks, duties and responsibilities.

**8.3** The Company Security Officer and appropriate shore-based company personnel, should have knowledge of, and receive training in, some or all of the following, as appropriate:

.1 security administration;
.2 relevant international conventions, codes and recommendations;
.3 relevant government legislation and regulations;
.4 responsibilities and functions of other security organizations;
.5 methodology of ship security assessment;
.6 methods of ship security surveys and inspections;
.7 ship and port operations and conditions;
.8 ship and port facility security measures;
.9 emergency preparedness and response and contingency planning;
.10 instruction techniques for security training and education, including security measures and procedures;
.11 handling sensitive security - related information and security-related communications;

.12 knowledge of current security threats and patterns;

.13 recognition and detection of weapons, dangerous substances and devices;

.14 recognition, on a non – discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with port facilities; and

.20 assessment of security drills and exercises.

**8.4** The Company Security Officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with the ISPS Code.

**8.5** The duties and responsibilities of the Company Security Officer shall also include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and cooperation between the Ship Security Officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirements;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

## 9 Ship Security Officer

**9.1** Ship Security Officers shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of the ISPS Code.

**9.2** The Ship Security Officer should have knowledge of, and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of ship security assessment;

.6 methods of ship security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

.13 recognition and detection of weapons, dangerous substances and devices;

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with port facilities;

.20 assessment of security drills and exercises;

.21 the layout of the ship;

.22 the ship security plan and related procedures (including scenario-based training on how to respond);

.23 crowd management and control techniques;

.24 operations of security equipment and systems; and

.25 testing, calibration and whilst at sea maintenance of security equipment and systems.

**9.3** The duties and responsibilities of the Ship Security Officer shall include, but are not limited to:

.1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.2 maintaining and supervising the implementation of the Ship Security Plan, including any amendments to the plan;

.3 coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

.5 reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

.6 enhancing security awareness and vigilance on board;

.7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.8 reporting all security incidents;

.9 coordinating implementation of the ship security plan with the Company Security Officer and the relevant port facility security officer; and

.10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

**9.4** Shipboard personnel having specific security duties shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of the ISPS Code.

**9.5** Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 crowd management and control techniques;

.6 security-related communications;

.7 knowledge of the emergency procedures and contingency plans;

.8 operations of security equipment and systems;

.9 testing, calibration and whilst at sea maintenance of security equipment and systems;

.10 inspection, control, and monitoring techniques; and

.11 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

**9.6** All other shipboard personnel shall have sufficient knowledge of and be familiar with relevant provisions of the ship security plan, including:

.1 the meaning and the consequential requirements of the different security levels;

.2 knowledge of the emergency procedures and contingency plans;

.3 recognition and detection of weapons, dangerous substances and devices;

.4 recognition, on a non – discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and

.5 techniques used to circumvent security measures.

## 10 Documentation

### 10.1 Ship security assessment

**10.1.1** Company Security Officers are responsible for undertaking ship security assessments.

**10.1.2** The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key shipboard operations that it is important to protect;

.3 identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and

.4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

**10.1.3** The ship security assessment should also address the following elements on board or within the ship:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks; and

.6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

## 10.2 Ship security plan

**10.2.1** Each ship shall carry on board a ship security plan approved by the Administration, unless exempted. The plan shall make provisions for the three security levels as defined in part A of the ISPS Code.

**10.2.2** The ship security plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats o r breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

.9 procedures for training, drills and exercises associated with the plan;

.10 procedures for interfacing with port facility security activities;

.11 procedures for the periodic review of the plan and for updating;

.12 procedures for reporting security incidents;

.13 identification of the Ship Security Officer;

.14 identification of the Company Security Officer including 24-hour contact details;

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided; and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

**10.2.3** The ship security plan shall be protected from unauthorized access or disclosure.

**10.2.4** Ship security plans should be reviewed annually, or following:

.1 a major security drill or exercise;

.2 a security threat or incident involving the ship;

.3 a change in shipping operations, including the operator;

.4 completion of a review of the ship security assessment;

.5 the identification, in an internal audit or inspection by the Administration, of failings in the ship's security operations, to the extent that the approved ship security plan may no longer be relevant.

## 11 Training, drills and exercises

### 11.1 Training

**11.1.1** The Ship Security Officer, the Company Security Officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of the ISPS Code.

**11.1.2** Shipboard personnel without designated security duties should receive security-related familiarization training to be able to:

.1 report a security incident;

.2 know the procedures to follow when they recognize a security threat; and

.3 take part in security - related emergency and contingency procedures.

### 11.2 Drills

**11.2.1** Drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances.

**11.2.2** Drills should be conducted at least once every three months. In addition, where more than 25% of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship within the last three months, a drill should be conducted within one week of the change.

**11.2.3** Drills may be defined as supervised activities that are used to test a single measure or procedure in the ship security plan.

**11.2.4** Shipboard drills should cover such scenarios as:

.1 identification and search of unauthorized visitors on board the ship;

.2 recognition of materials that may pose a security threat;

.3 methods to deter attackers from approaching the ship;

.4 recognition of restricted areas; and

.5 mustering for evacuation.

**11.3.1** Exercises

**11.3.1** The Company Security Officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals.

**11.3.2** Exercises should be carried out at least once each calendar year with no more than 18 months between the exercises.

**11.3.3** Exercises are more complex activities which test several measures and procedures at the same time.

**11.3.4** Exercises should test communications, coordination, resource availability, and response. Exercises may be:

.1 full scale or live;

.2 table top simulation or seminar; or

.3 combined with other exercises held such as search and rescue or emergency response exercises.

## 12 Physical security

### 12.1 Restricted areas

**12.1.1** The ship security plan shall address the identification of the restricted areas and measures for the prevention of unauthorized access to them.

**12.1.2** The ship security plan should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 prevent unauthorized access;

.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;

.3 protect sensitive security areas within the ship; and

.4 protect cargo and ship's stores from tampering.

**12.1.3** Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in SOLAS chapter XI-2;

.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

.3 ventilation and air – conditioning systems and other similar spaces;

.4 spaces with access to potable water tanks, pumps, or manifolds;

.5 spaces containing dangerous goods or hazardous substances;

.6 spaces containing cargo pumps and their controls;

.7 cargo spaces and spaces containing ship's stores;

.8 crew accommodation; and

.9 any other areas as determined by the Company Security Officer, through the ship security assessment to which access must be restricted to maintain the security of the ship.

## 12.2 Access points

**12.2.1** The ship security plan shall address measures for the prevention of unauthorized access to the ship, including boarding of a ship when in port or at sea.

## 12.3 Signage

**12.3.1** The ship security plan should ensure that all restricted areas should be clearly marked, indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

### 12.4 Identification

**12.4.1** The ship security plan should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge.

### 12.5 Lighting

**12.5.1** The ship should have lighting sufficient to monitor the ship, the restricted areas on board and areas surrounding the ship.

### 12.6 Surveillance

**12.6.1** The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of: watchkeepers, security guards and deck watches including patrols.

**12.6.2** Administrations should require that security equipment receive regular maintenance checks and that these checks be recorded. Security equipment can include:

.1 closed-circuit television (CCTV) and lighting;
.2 communications and x-ray equipment;
.3 archway and hand-held metal detectors;
.4 perimeter/intruder detection systems;
.5 automated access control equipment;
.6 information, including computer, security; and
.7 explosive trace and vapour detection equipment.

### 12.7 Communications

**12.7.1** Ship Security Officers intending to use a port facility should maintain effective communication with the Port Facility Security Officers (PFSOs).

## 13 Operational security

### 13.1 Master's discretion

**13.1.1** The master shall not be constrained from taking or executing any decision which, in the professional judgment of the master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

**13.1.2** If, in the professional judgment of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship.

## 13.2 Port Control Compliance

**13.2.1** Every ship intending to enter a port facility of [State] shall provide the security information requested by the officers duly authorized by that government. The master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

## 13.3 Manning requirements

**13.3.1** In establishing the minimum safe manning of a ship the Administration should take into account any additional workload which may result from the implementation of the ship security plan and ensure that the ship is sufficiently and effectively manned.

## 13.4 Access control

**13.4.1** Ship security plans shall address measures for the prevention of unauthorized access to the ship.

## 13.5 Cargo operations

**13.5.1** Security measures relating to cargo handling should:

.1 prevent tampering; and

.2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

**13.5.2** Cargo entering the port facility should have adequate and reliable documentation, which is standardized, matches the cargo with the conveyance transporting it to the port facility, is resistant to forgery and is consistently examined by security personnel prior to allowing admittance onto the port facility.

## 13.6 Ship's stores

**13.6.1** Security measures relating to the delivery of ship's stores should:

.1 ensure the integrity of ship's stores;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering; and

.4 prevent ship's stores from being accepted unless ordered.

**13.6.2** Ship's stores entering the port facility should have adequate and reliable documentation, which is standardized, matches the ship's stores with the conveyance transporting it to the port facility, is resistant to forgery and is consistently examined by security personnel prior to allowing admittance onto the port facility.

### 13.7 Unaccompanied baggage procedures

**13.7.1** The ship security plan should establish 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) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship.

## 14 International Ship Security Certificate (ISSC)

**14.1** Ships shall carry on board either the International Ship Security Certificate or, in limited circumstances, the Interim International Ship Security Certificate, both of which are issued by DMA.

**14.1.1** An Interim International Ship Security Certificate shall only be issued when the Administration or recognized security organization, on behalf of the DMA, has verified that:

.1 the ship security assessment required by the ISPS Code has been completed;

.2 a copy of the ship security plan meeting the requirements of SOLAS chapter XI-2 and part A of the ISPS Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;

.3 the ship is provided with a ship security alert system meeting the requirements of SOLAS regulation XI-2/6, if required;

.4 the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in part A of the ISPS Code; and

.5 the Ship Security Officer meets the requirements of part A of the ISPS Code.

**14.1.2** Administrations or RSOs may issue an Interim Issue when:

.1 a ship is on delivery, or prior to its entry or re-entry into service;

.2 a SOLAS ship is changing its flag;

.3 a ship is being transferred from a non-SOLAS State;

.4 the shipping company operating a SOLAS ship changes.

**14.1.3** An Interim Issue can only be issued when the Administration or RSO has conducted interim verification confirming that:

.1 the ship's SSA has been completed;

.2 there is a copy of the SSP on board;

.3 the SSP has been submitted for review and approval and is being implemented;

.4 the ship has a ship security alert system (SSAS);

.5 threshes ensured that the necessary arrangements are in place, including drills, exercises and internal audits, for the ship to successfully complete the required verification within six months;

.6 arrangements are in place to carry out the required verification;

.7 the master, SSO and other personnel with specific security duties are familiar with their responsibilities in the Maritime Security Measures and SSP and have been provided with such information in the ship's working language or in a language they understand;

.8 the SSO meets the relevant requirements in the Maritime Security Measures.

**14.1.4** Following verification of the items listed above, an Interim Issues valid for up to six months.

**14.1.5** If a full Issues issued to the ship during that six-month period, the Interim ISSC is revoked.

**14.1.6** An Interim ISSC cannot be extended.

**14.1.7** An Administration shall not issue a subsequent or consecutive Interim ISSC if it believes that the shipping company intends to avoid full compliance with the Maritime Security Measures for a period beyond the initial six-month validity of the initial Interim ISSC.

**14.1.8** ISSCs and Interim ISSCs can be inspected as part of control and compliance measures described in subsection 4.10 of Guide to Maritime Security and the ISPS Code.

**14.1.9** An ISSC must be issued for a period specified by the Administration which, with one exception, can not exceed five years. The exception covers the situation when a renewal verification is completed within three months of the expiry date of the existing ISSC. In this situation, the new ISSC becomes valid from the date of completion of the renewal verification to a date not exceeding five years from the expiry date of the existing ISSC.

**14.1.10** An ISSC shall only be issued or renewed when:

.1 the ship has an approved SSP indicating that it fully addresses all requirements specified in the Maritime Security Measures, as outlined in paragraphs 4.8.1 to 4.8.11, and

.2 the Administration is satisfied, based on objective evidence, that the ship is operating in accordance with the provisions in the approved SSP.

**14.1.11** A Certificate shall not issue in cases where there is a minor deviation from the SSP, even when the ship's ability to operate at security levels 1 to 3 is not compromised.

**14.1.12** A Certificate can be issued or endorsed by:

.1 the Department of Marine Administration;

.2 an RSO authorized to act on behalf of the Department of Marine Administration; or

.3 another Administration acting on behalf of the Department of Marine Administration.

**14.1.13** An International Ship Security Certificate shall not be valid for more than five years.

**14.1.14** A ship which is not normally engaged on international voyages but which, in exceptional circumstances, is required to undertake a single international voyage may be exempted by DMA from any of the requirements of the present regulations provided that it complies with safety requirements which are adequate in the opinion of DMA for the voyage which is to be undertaken by the ship.

## 14.2 Verifications

**14.2.1** SOLAS ships are subject to verifications of their compliance with the Maritime Security Measures.

**14.2.2** Before a ship is put into service and before an Interim ISSC is issued, an interim verification takes place. Although the ISPS Code refers to this type of verification as an 'initial verification', it has become standard industry practice to-use the term 'interim verification'.

**14.2.3** Subsequent verifications that take place are:

.1 before an ISSC is issued - an *initial verification;*

.2 at least once between the second and third anniversary of the Issuance of the ISSC if the validity period is for five years - an *intermediate verification;*

.3 before the ISSC is renewed - a *renewal verification;* and

.4 at other times, at the discretion of the Administration.

**14.2.4** The appropriate level of thoroughness in the verification of security systems should be as follows:

.1 100% verification for all technical equipment specified in the SSP; and

.2 a sample audit for all operational (non-technical) security measures, to a level necessary for the auditor to verify the whole operating system.

**14.2.5** An initial verification is conducted to ensure that the ship's security system and any security equipment required by the Maritime Security Measures and the approved SSP is in satisfactory condition and fit for the service for which the ship is intended.

**14.2.6** An intermediate verification is conducted to ensure that the ship's security system and any security equipment required by the Maritime Security Measures and the SSP remains in satisfactory condition and is fit for the service for which the ship is intended.

**14.2.7** A renewal verification is to ensure the ship's security system and any security equipment fully complies with the requirements of the Maritime Security Measures and the approved SSP, is in satisfactory condition and is fit for the service for which the ship is intended.

**14.2.8** After verification, the ship's security system and security equipment should be maintained to conform with the provision of the Maritime Security Measures. No changes can be made to ten security system or security equipment or to the approved SSP unless agreed by the Administration.

**14.2.9 Duration of validity**

**14.2.9.1** The duration of a renewed five-year Issue can vary depending on the date that the renewal verification takes place. If it is completed:

.1 within the three months before the expiry of the original ISSC, then the next five-year period starts at the original expiry date;

.2 after the expiry of the original ISSC, then the next five-year period starts at the original expiry date;

.3 more than three months before the expiry of the original ISSC, then the next five-year period starts at the date of completion of the renewal verification.

**14.2.9.2** If an ISSC has been issued for a period of less than five years, an Administration can extend its validity to a maximum of five years after undertaking the required verification.

**14.2.9.3** If a new Issue cannot be placed on the ship before the original Issue expires, the Administration can endorse the original Issue for an extended period not exceeding five months. The new five-year period starts at the original expiry date.

**14.2.9.4** If a ship is in transit, or its arrival at the port where verification is to take place is delayed, the Administration can endorse the original Issue to allow the ship to complete its voyage. However, the validity period cannot be extended for longer than three months and the new five-year period starts at the expiry date set for the original ISSC.

**14.2.9.5** If a ship is engaged on short voyages, its Issue can be extended for a period of up to one month with the new five-year period starting at the expiry date of the original ISSC.

**14.2.9.6** If an intermediate verification is undertaken before the second anniversary of issuance of an Issue that is valid for five years, its validity period must be reduced to show an expiry date that is no more than three years after the completion date of the verification. However, the original expiry date can be maintained with a further intermediate verification.

## 14.3 Loss of validity

**14.3.1** An Issue can lose its validity when:

.1 the required intermediate and renewal verifications have not taken place;

.2 it has not been endorsed following an intermediate verification;

.3 a new shipping company takes over the operation of the ship; or

.4 the 'ship changes its flag.

**14.3.2** On changes of flag, the original Administration should provide the new Administration with copies of all relevant information on the ship's ISSC, including copies of available verification reports.

## 14.4 SHIP SECURITY AUDITS

**14.4.1** The procedure for security audits outlined in the following paragraphs include all steps relevant for initial verification. Ship Security audits for the interim, intermediate, additional and renewal verification shall be based on the same principles, even if there scope may be different.

### 14.4.2 Application for Audit

The company shall submit a request for audit to the Department of Marine Administration ( DMA ) or to the organization recognized by the Administration for issuing a International Ship Security Certificate or a Interim International Ship Security Certificate on behalf of the Administration. The Administration or the recognized organization shall then nominate the lead auditor and, if relevant, the audit team.

### 14.4.3 Preparing the audit

**.1** The auditor shall review the relevant security performance records of the ship and take them into consideration when preparing **audit plan** ( form ISPS/Audit Plan ) which is to be flexible in order to permit changes in emphasis based on information gathered during the audit, and to permit the effective use of resources.

**.2** The nominated lead auditor shall liaise with the company and produce an audit plan. The audit plan shall include:

**.1** Identification of the individuals having significant direct responsibilities regarding the SSP.

**.2** Identification of reference documents associated with the SSP.

**.3** Identification of auditor (s).

**.4** The language of the audit.

**.5** Identification of organizational units to be audited.

**.6** The date and place where the audit is to be conducted.

**.7** The schedule of meetings to be held with Company's management.

**.8** Audit report distribution.

**.9** The Administration or the recognized organization should Conduct external audit between the second and third anniversary dates for ISSC.

**.3** The auditor shall provide the working documents which are to govern the execution of the audit in order to facilitate the assessments, investigations and examinations in accordance with the standard procedures, instructions and forms which have been established to ensure consistent auditing practices.

**.4** The audit team shall be able to communicate effectively with auditees.

### 14.2.5 Executing the audit

The audit is to start with an opening meeting in order to:

**.1** Introduce the auditor (s) to the Senior of Company Management and Ship's Management. Explain the scope and objective of the audit Provide a short summary of the methods and procedures to be used to conduct the audit Establish the official communication line between the auditor (s) and the Company and/or the ship.

**.2** Confirm that resources, documentation and facilities needed to perform the audit are available.

**.3** Confirm the time and date of the closing meeting and clarify possible unclear details relevant to the audit.

**.4** The auditor (s) is to review the SSP on the basis of the documentation presented by the company and objective evidence of its effective implementation, which shall be collected through interviews and examination of documents. Observation of activities and Conditions may also be included when necessary to determine the Effectiveness of the SSP in meeting the specific standards of Security required by the ISPS Code.

**.5** Audit observations are to be documented in a clear, concise manner and supported by objective evidence. These shall be reviewed by the auditor(s) in order to determine which are to be reported as major non - conformities, non - conformities, observations or findings.

**.6** At the end of the audit, prior to preparing the audit report, the auditor (s) is to hold a meeting with the senior management of the Company or Ship and those responsible for the functions concerned. The purpose is to present major non-conformities, non- conformities, Observations and findings to the Company's and/or ships management, in such a manner so as to ensure that they clearly understand the results of the audit.

### 14.2.6 Audit Report

The **Audit report** (form ISPS/Audit Report) is to be prepared by the Lead Auditor, based on information gathered by and discussed with the audit team members (if applicable). It must be accurate and complete, reflecting the content of the audit, and is to include the following items, as applicable

**.1** Company's and/or ship particulars

**.2** The date of completion of the audit and submission of the audit report

**.3** The scope and objectives of the audit.

**.4** Details of the audit plan, auditor (s), Company's representatives and a list of all organizational units audited; and

**.5** All major non-conformities, non-conformities, observations and findings

**.6** Auditor recommendations

The audit report is to be submitted to the Company, which should be advised to provide the ship with a copy of the relevant Security audit report.

# 15 Security obligations

## 15.1 Communications / reporting procedures

**15.2.1** Ships intending to enter ports of Myanmar may be required to provide the following information prior to entry into port:

.1 that the ship possesses a valid certificate and the name of its issuing authority;

.2 the security level at which the ship is currently operating;

.3 the security level at which the ship operated in any previous port where it has conducted a ship/port interface within a specified time frame;

.4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within a specified time frame;

.5 that the appropriate ship security procedures were maintained during any ship-to-ship activity within a specified time frame; or

.6 other practical security-related information (not to include details of the ship security plan).

**15.2.2** Examples of other practical security-related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

.1 information contained in the continuous synopsis record;

.2 location of the ship at the time the report is made;

.3 expected time of arrival of the ship in port;

.4 crew list;

.5 general description of cargo aboard the ship;

.6 passenger list; and

.7 information required to be carried under SOLAS regulation XI-2/5.

**15.2.3** DMA may specify the minimum time before arrival in port that a ship should notify its intention to arrive and provide the necessary security-related information. The time can vary between 24 and 96 hours prior to arrival.

**15.2.4** The master may decline to provide such information, but failure to do so may result in denial of entry into port.

## 16 Incident response

### 16.1 Security incidents

**16.1.1** DMA is required to specify the types of security incident that have to be reported to them. In such cases, they should provide guidance on their timing, procedures to be followed and their distribution. They should include reporting incidents to local law-enforcement agencies when in a port facility or the adjacent coastal State.

**16.1.2** Security incidents generally can fall into two categories:

**16.1.2.1** those considered to be sufficiently serious that they should be reported to relevant authorities by the Company Security Officer, including:

.1 unauthorized access to restricted areas within the ship for suspected threat-related reasons;

.2 unauthorized carriage or discovery of stowaways, weapons or explosives;

.3 incidents of which the media are aware;

.4 bomb warnings;

.5 attempted or successful boardings; and

.6 damage to the ship caused by explosive devices or arson.

**16.1.2.2** those of a less serious nature but which require reporting to, and investigation by, the Ship Security Officer can include:

.1 unauthorized access to the ship caused by breaches of access control points;

.2 inappropriate use of passes;

.3 damage to equipment through sabotage or vandalism;

.4 unauthorized disclosure of a ship security plan;

.5 suspicious behaviour near the ship when at a port facility;

.6 suspicious packages near the ship when at a port facility; and

.7 unsecured access points to the ship.

## 16.2 Unauthorized access/breach procedures

**16.2.1** Ship security plans shall address procedures for responding to security threats or breaches of security, including:

.1 provisions for maintaining critical operations of the ship or ship/port interface; and

.2 procedures for reporting security incidents.

## 17 Best management practices

**17.1** The Company Security Officer is encouraged to ensure that a ship security plan is in place for passage through high security risk areas, and that this is exercised, briefed and discussed with the Master and the Ship Security Officer.

**17.2** The provision of carefully planned and installed ship protection measures prior to transiting the high risk area is very strongly recommended.

**17.3** Ship security plans should include specific guidelines on the use of weapons in the vicinity of dangerous goods or hazardous substances. Firearms carried on board ship may have to be reported on arrival in port and may have to be surrendered, or held securely, for the duration of the port visit.

# Department of Marine Administration
# AUDIT PLAN

Type of Audit : ISPS/Audit Plan

Name of Company / Ship :

Conducted Date of Audit : Place :

| Date / Time | Agendum | Interviews / Person Involves |
|---|---|---|
| | Opening Meeting | Auditor |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Closing Meeting / Review | Auditor |
| | | |
| | | |
| | | |

Name of Auditors :

Signature :

Date :

| | |
|---|---|
| | **Department of Marine Administration**<br>**ISPS Code compliance verification audit report**<br>**Page 1 of 2** |

## ISPS/ Audit Report

Type of audit :SSP Approval/ Interim / Initial/ Intermediate/ Renewal/ Additional

| | | | |
|---|---|---|---|
| Name of Vessel | | IMO No. | |
| Type of vessel | | Location | |
| Company: | | | |

| | | | |
|---|---|---|---|
| Audit start time | hrs/ dd-mm-yyyy | Audit completion time | hrs/ dd-mm-yyyy |
| SSP approved by | | Date approved | dd-mm-yyyy |
| Opening meeting commence | hrs/ dd-mm-yyyy | Attendees | Master, C/O,2/O(SSO), C/E and CSO |
| Audit findings | NCNs- Nil | Observations | Nil |
| Last internal security audit date | dd-mm-yyyy | | |
| Last SSP review | dd-mm-yyyy | | |
| CSR | | | |
| Maintenance of security equipment | | | |
| Training and drills | Last Security Exercise :dd-mm-yyyy<br>Last Security Drill :dd-mm-yyyy | | |

Audit report

Opening meeting was conducted with the following attendees:

The closing meeting was conducted with same attendees as the opening meeting.

| | | |
|---|---|---|
| Auditor<br>Company Official/ Master | | |

| | |
|---|---|
| | **Department of Marine Administration**<br><br>**ISPS Code compliance verification**<br>**Non-conformity report**<br><br>**Page 1 of 1** |

**ISPS/ NCR**

Type of audit :SSP Approval/ Interim / Initial/ Intermediate/ Renewal/ Additional

Name of Office/ Vessel : _____ IMO No./ Company unique No._____

Type of vessel: _____ Location: _____

Company: _____

| | | | |
|---|---|---|---|
| Area of deficiency<br>Maintenance | ISPS element reference | | Note number |
| Date of issue:<br>dd-mm-yyyy | Date for completion:<br>dd-mm-yyyy | N.C No. | Xx |
| Narrative | | | |
| Date | Signature of Auditor | | |

## 18 Forms of Certificates

**18.1** Forms of the International Ship Security Certificate or Interim International Ship Security Certificate shall be drawn up under this Guidance.

**INTERNATIONAL SHIP SECURITY CERTIFICATE**
**The Government of The Republic of the Union of Myanmar**

***Certificate No. DMA/ISSC/xxx-yy***



Issued under the provisions of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND PORT FACILITIES (ISPS CODE)

***Under the authority of the Government of Union of Myanmar by Department of Marine Administration***

Name of Ship: ……..
Distinctive number or letters: ……..
Port of registry: ……..
Type of ship: ……..
Gross tonnage: ……
IMO Number: ……
Name and address of the Company: ……
……
……..
Company identification number: ……

THIS IS TO CERTIFY :

1. that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;
2. that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;
3. that the ship is provided with an approved ship security plan.

Date of initial/renewal verification on which this Certificate is based…… This Certificate is valid until ……, subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at……
( Place of issue of the Certificate)
Date of issue……

Director General
Department of Marine Administration

(seal or stamp of issuing authority, as appropriate)

**Endorsement for intermediate verification**

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate verification

Signed:……..
( Signature of authorized official )

Place: ……..

Date: ……..

(seal or stamp of authority, as appropriate)

***Endorsement for additional verifications****

Additional verification

Signed:…….
( Signature of authorized official )

Place: ……

Date: ……

(seal or stamp of authority, as appropriate)

Additional verification

Signed:……
( Signature of authorized official )

Place:……..

Date: ……

(seal or stamp of authority, as appropriate)

Additional verification

Signed:……
( Signature of authorized official )

Place: ……

Date: ..……

(seal or stamp of authority, as appropriate)

* This part of the certificate shall be adapted by the Administration to indicate whether it has established additional verifications as provided for in section 19.1.1.4. of part A of the ISPS Code

***Additional verification in accordance with section A/ 19.3.7.2 of the ISPS Code***

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Signed:…….
( Signature of authorized official )

Place: …….

Date:……

(seal or stamp of authority, as appropriate)

***Endorsement to extend the certificate if valid for less than 5 years where section A/ 19.3.3 of the ISPS Code applies***

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until ……..……

Signed:……...
( Signature of authorized official )

Place: ……..

Date: ……

(seal or stamp of authority, as appropriate)

***Endorsement where the renewal verification has been completed and section A/ 19.3.4 of the ISPS Code applies***

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until ……..

Signed:……
( Signature of authorized official )

Place: …….

Date: ……

(seal or stamp of authority, as appropriate)

***Endorsement to extend the validity of the certificate until reaching the port of verification where section A/ 19.3.5 of the ISPS Code applies or for a period of grace where section A/ 19.3.6 of the ISPS Code applies***

The certificate shall, in accordance with section 19.3.5 / 19.3.6* of part A of the ISPS Code, be accepted as valid until ……..

Signed:……

( Signature of authorized official )

Place: ……

Date: ……

(seal or stamp of authority, as appropriate)

***Endorsement for advancement of expiry date where section A/19.3.7.1 of the ISPS Code applies***

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date† is ……

Signed:……

( Signature of authorized official )

Place: ……

Date: ……

(seal or stamp of authority, as appropriate)

* Delete as appropriate

† In case of completion of this part of the Certificate , the expiry date shown on the front of the Certificate shall also be amended accordingly.

**INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE**

## The Government of The Republic of the Union of Myanmar

***Certificate No. DMA/ IISSC/xxx-yy***



Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND PORT FACILITIES (ISPS CODE)

***Under the authority of the Government of Union of Myanmar***
***by Department of Marine Administration***

Name of Ship: ……..……..

Distinctive number or letters: ……..……..

Port of registry: ……..……..

Type of ship: ..……..

Gross tonnage: ……..……

IMO Number: ……..……

Name and address of the Company ……

……

……

Company identification number: ……

Is this a subsequent, consecutive Interim Certificate? Yes/No*

If Yes , date of issue of initial Interim Certificate: ……

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until ……

Issued at……

( Place of issue of the Certificate)

Date of issue……

Director General
Department of Marine Administration

( seal or stamp of issuing authority, as appropriate)

* Delete as appropriate.