Table of Contents

EXPLANATORY NOTE

The tragic events of September 11th 2001 on the US World Trade Center necessitated the twenty-second session of the Assembly of the International Maritime Organization[1], in November 2001. The Assembly unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea,[2]1974(known as the Diplomatic Conference on Maritime Security) in December 2001. The motivation for this step taken by the IMO was the consideration of a possible attack on ships and/or ports considering their economic vitality to international commerce and strategic locations at the entrance to the national territories of countries respectively. Acts of terrorism and armed robbery and piracy against ships and ports are also threats to the international security and peace of the world.

Outrage in the shipping industry at the alarming growth in piracy on the world's oceans prompted the creation of the International Maritime Bureau Piracy Reporting Center[3] in 1992 in Kuala Lumpur. Piracy and armed robbery against ships and the potential for terrorist attacks on vulnerable sea shipping threaten the growth of the Asia-Pacific region and disrupt the stability of global commerce[4], particularly as these have become tools of transnational organized crimes: maritime security is an indispensable and fundamental condition for the welfare and economic stability of all countries, and ensuring this security is in the interest of all countries.[5]

It is of particular interest for a country like Cameroon whose major port is situated along the West African coast and at a strategic position in Central Africa to adopt, incorporate, and implement the security measures as provided in the International Code for the Security of Ships and of Port Facilities.[6]The main port of Cameroon, the Douala

[1] Hereinafter referred to as the IMO.
[2] Hereinafter referred to as SOLAS
[3] The center is financed by voluntary contributions from a number of companies and provides its services free of charge to all vessels irrespective of ownership or flag.
[4] The recent growth of the economies of the Asian region has an impact on global commerce which if disrupted will affect the whole world negatively.
[5] Declaration of the Chairman of the ASEAN Regional Forum on June 17th 2003.
[6] Hereinafter referred to as the ISPS Code.

port, serves the landlocked countries of the region, which are, Chad and the Central African Republic. The port also acts as a transshipment port for cargoes destined to the ports of Gabon, Equatorial Guinea and the Republic of Congo, whose ports are significantly smaller to accommodate the large vessels that normally call at the port of Douala. The recent construction of the Chad-Cameroon pipeline adds to the value-added logistics services provided by the dedicated oil terminals in the ports of Limbe and Kribi and therefore an increased requirement for stringent security measures for the detection and prevention of any security incident.

Any form of terrorist attack or undetected threat to the security of the ports of Cameroon or to any ship destined to any of the ports in Cameroon, or within Cameroon's territorial waters will have drastic socio-economic and political effects, which will spread to the other States of the region, because of the importance of the ports of Cameroon to the international trade and exchange of the States of the sub-region.

The ratification of the SOLAS Convention by Cameroon gives the Convention the force of law and automatically brings it into force. This is so because Cameroon is a monist State and no secondary legislation is required for a convention that has been ratified to enter into force. For the additional security measures due to the geographical and structural requirements of the ports of Cameroon, like any other ports in the developing countries of Africa, south of the Sahara, the ISPS Code has to be incorporated as a separate legislative text so as to take into consideration these differences, which were not contemplated in the Code: the ports of Cameroon are not as developed as the ports of the developed countries. Provisions in the ISPS Code reflect the technologically sophisticated equipments to be used in the detection of dangerous and unwanted materials in the port areas, but the lack of this technology and the structural layout of the ports of Cameroon require physical presence and surveillance of port operations to detect and deter any dangerous activities in the ports which can lead to a security incident in the ports.

Although the attack on the World Trade Center in September 2001 marked the watershed in the progress to international consensus, some work had been done beforehand. In December 1972, the General Assembly of the United Nations set up an ad

hoc Committee on Terrorism[7] and in 1994 a Declaration on Measures to Eliminate International Terrorism was adopted.[8] In Resolution 1368(2001) adopted the day following the September 11 attacks, the Security Council, noting that it was "Determined" to combat by all means threats to international peace and security caused by terrorist attack, unequivocally condemned the attack and declared that it regarded such attack like any act of international terrorism. This upheld the view in the earlier Resolution 1373, including the preparation of model laws, directing States on measures to be adopted and enforced in the detection and deterrence of acts of piracy and terrorism threatening ships and port facilities, as appropriate, and to examine the availability of various technical, financial, legislative and other programmes to facilitate the implementation of Resolution 1373[9].

The SUA (Rome) Convention 1988[10] that falls within the purview of the purposes and principles of the charter of the United Nations alludes to the maintenance of International peace and security and the promotion of friendly relations and co-operation among nations. Unlawful acts against the safety of maritime navigation jeopardize the safety of persons and property, and seriously affect the operation of maritime services and undermine the confidence of the people of the world in the safety of maritime navigation. All these are contributory factors for the enactment of the ISPS Code.

> "…Attempts to attack the problem of piracy and maritime violence by proposing a more systematic treatment of these serious problems through national law, under whose admiralty/maritime jurisdiction the great majority of relevant incidents fall. The intention of the Working Group[11] is to present a series of ideas designed to

[7] General Assembly Resolution 3034(xxvii)
[8] General assembly Resolution 49/60-This condemned "all acts, methods, and practices of terrorism, as criminal and unjustifiable, wherever and by whomever committed", noting that, "criminal acts intended or calculated to provoke a state of terror in the general public, a group or person or persons or particular persons for political purposes or any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."-International Law by Malcolm SHAW, 5th Ed, CAMBRIDGE UNIVERSITY PRESS.
[9] Report of the Government of Canada to the Counter-Terrorism Committee of the United Nations. And its determination to collaborate in the fight against terrorism and to apply stricter measures in the prevention of acts of terrorism.
[10] The Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation.
[11] The following Model National Law on Acts of Piracy and Maritime Violence is the result of deliberation by this Joint Working Group on uniformity of law concerning Acts of Piracy and Maritime Violence. The Working Group is composed of representatives of the following international organizations; the Comite maritime International (CMI), the Baltic and International maritime Council (BIMCO), the International Chamber of Shipping (ICS), the International Criminal Police Organization (INTERPOL), the

> achieve greater uniformity in the body of various national legal traditions rather than producing a standardized document. Penalties are not specified, but must be severe enough in the context of national criminal law to discourage illegal conduct. It is recognized that those governments undertaking a review of piracy and related laws possess particular expertise in their own national problems…"[12]

This approach was immediately copied by the IMO and the amendment to SOLAS adopted the ISPS Code as a mandatory legislation to help in the detection and prevention of acts of terrorism and piracy, which are potential threats and hazards to the port facilities, and ships respectively.

The ISPS Code and the Model laws have provided for guidelines, which countries not endowed with the expertise, like Cameroon, should emulate in the enactment of its own laws. These laws should bind all the parties involved in the maritime operations of Cameroon so as to contribute in the detection and deterrence of acts of terrorism and maritime violence. This Act for the Incorporation of the International Code for the Security of Ships and of Port Facilities (the ISPS Code) into the laws of Cameroon is composed of two Parts. Part A contains mandatory security provisions which must be complied with, and Part B contains Recommendations, which provides for guidelines for the compliance with Part A of the Act. Part B of this Act is drafted, taking into consideration, the geographically sensitive location of the ports in Cameroon and the unavailability of modern technology to detect and deter any acts of piracy or terrorism against ships in the territorial waters of Cameroon or the port facilities. This Part of this Act is not mandatory, but it considers the situation of the ports in Cameroon as they are and provides for pragmatic and useful guidelines that should be adopted so as to direct the Government in the implementation of the mandatory provisions of Part A of the Act.

The ISPS Code from which most of the provisions Act is sourced has its merits. Though in force only for a few months now- 1 July 2004, the ISPS Code is a police measure against acts of terrorism and piracy, which threaten the security of ships and port facilities. Its entry into force and the implementation of its provisions by most States has

---

International Group of P&I Clubs (IGP&I), the International Chamber of Shipping (ICC), the International maritime Bureau (IMB), the International maritime Organization (IMO), the International Transport Workers Federation (ITF), the International Union of Marine Insurance (IUMI), and the United Nations (Office of Legal Affairs / Division of Ocean Affairs and the Law of the sea) (UN OLA / DOALOS).

[12] Preamble of the Model National Law on Acts of Piracy and Maritime Violence, Comite Maritime International, London, December 7, 2001.

helped in the identification of the most susceptible targets that could be attacked by terrorists or pirates. Measures have been put in place in the provisions of the Code to prevent any potential attacks on such structures. Since the entry into force of the Code on 1 July 2004 there has been no major security incident anywhere in the world.

As a signatory to the SOLAS Convention, Cameroon has to implement and enforce the provisions of the ISPS code, taking into consideration Cameroon's scientific and technological, geographical, economic and political realities. This will guarantee Cameroon's gradual and progressive move in its struggle towards meeting the IMO standards of SAFE, SECURE AND EFFICIENT SHIPPING ON CLEAN OCEANS.

AN ACT FOR THE INCORPORATION OF THE INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES INTO THE LAWS OF CAMEROON

This Act shall enter into force on such a day, as the Parliament shall decide.

PREAM BLE

THE GOVERNMENT OF CAMEROON,

RECALLING Article 15(j) of the Convention on the International Maritime Organization, of which Cameroon is a member, concerning the functions of the Assembly in relation to regulations and guidelines concerning Maritime Safety,

RECALLING ALSO the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation 1988,

RECOGNIZING WITH DEEP CONCERN the grave danger to safety of life at sea, Maritime security and the prevention of pollution of the marine environment arising from acts of piracy and armed robbery against ships,

NOTING RESOLUTION A/RES/55/7 on Oceans and the Law of the Sea, by which the United Nations General Assembly, at its fifty-fifth session, urged all States, and in particular coastal States, in affected regions to take all necessary and appropriate measures to prevent and combat incidents of piracy and armed robbery at sea, including through regional co-operation, and to investigate or co-operate in the investigation of such incidents wherever they occur and bring the alleged perpetrators to justice in accordance with international law,

BEING AWARE of the strategic location of the ports of Cameroon along the central part of the West African coast, and the economic impact of the ports to the development of the economy of the Central African Sub-region,

CONSIDERING Cameroon’s cultural diversity and ethnic multiplicity and strong economic ties with the land-locked States of the Central African Sub-region, and the political and economic crises that characterize the region,

RECOGNIZING the desire to bring Cameroon in line with the standards of maritime safety, security, and marine environment protection as prescribed by the International Maritime Organization,

HEREBY incorporates the International Code for the Security of Ships and of Port Facilities into the domestic laws of the State as the CAMEROON MARITIME SECURITY ACT, 2005.

Nothing in this Act shall preclude either the Government, the Port Authorities, or the shipping companies, operating in Cameroon, from requesting a security measure which is not provided in this Act, if the measure requested is deemed to be necessary for the prevention of an imminent security incident which the requesting body considers to be a possible threat to its security. Requests for additional security measures of this kind must be communicated to all the relevant authorities concerned with the application of this Act and appropriate collaboration is mandatory to address such a situation.

I GENERAL

I.1 The Short Title of this Act shall be the Cameroon Maritime Security Act 2005.

I.2 Introduction

This part of the Cameroon Maritime Security Act contains mandatory provisions to which reference is made in Part A of the International Code for the Security of Ships and of Port Facilities (The ISPS CODE) 2002.

I.3 Objectives

The objectives of this Act are;

1. to provide security measures which are intended to maintain an acceptable level of risk at all security levels;

2. to devise security measures which will reduce risks and in the main revolve around procedures to establish and control access to restricted areas and other vulnerable or sensitive key points, locations, functions or operations in the port;

3. to establish a framework of co-operation involving the Government, Government agencies, local administrations, and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities in Cameroon;

4. to establish the roles of the Government, Government agencies, local administrations and the shipping and port industries, at the national and international level, for ensuring maritime security;

5. to ensure the early and efficient collection and exchange of security-related information;

6. to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and

7. to ensure confidence that adequate and proportionate maritime security measures are in place.

I.4 Functional Requirements

In order to achieve its objectives, this Act embodies a number of functional requirements. These include, but are not limited to:

1. gathering and assessing information with respect to security threats and exchanging such information with all the appropriate maritime operators;

2. requiring the maintenance of communication protocols for ships and port facilities;

3. preventing unauthorized access to ships, port facilities and their restricted areas;

4. preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

5. providing means for raising the alarm in reaction to security threats or security incidents;

6. requiring ship and port facility plans based upon security assessments; and

7. requiring training, drills and exercises to ensure familiarity with security plans and procedures.

II DEFINITIONS

II.1 For the purpose of this Act, unless provided otherwise;

1. Act refers to this Act for the Incorporation of the ISPS Code into the laws of Cameroon (the Cameroon Maritime Security Act 2005).

2. The Government means the Government Ministry, Government agency, or local Administrative Authority in charge of maritime affairs in Cameroon.

3. The Code means the International Code for the Security of Ships and of Port. Facilities (the ISPS Code).

4. The Company means any company duly incorporated in Cameroon, which can either be a shipping company, port agency, time, voyage or bareboat charterer, or any other company having to deal with the reception and management of ships in Cameroonian ports.

5. Port facility security plan 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.

6. Ship security plan 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.

7. Ship security officer means the person on board the ship, accountable to the master, 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.

8. Company security officer 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.

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

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

11. 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.

12. 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.

II.2 The term “ship”, when used in this Act, includes mobile offshore drilling units and high-speed craft as defined in the ISPS Code.
II.3 “Government” in connection with any reference to a port facility, when used in this Act includes a reference to the designated authority.

II.4 Terms not defined in this Act shall have the same meaning as attributed to them in the ISPS Code.

III SCOPE OF APPLICATION

III.1 This Act shall apply to;

1. the following types of ships engaged in international voyages;

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

ii. cargo ships, including high-speed craft, of 500 gross tonnage and above;

iii. mobile offshore drilling units; and

2. port facilities serving such ships engaged on international voyages.

III.2 Notwithstanding the provisions of section III.1.2 the Government shall decide the extent of application of this Act to those port facilities within the country which, although used primarily by ships engaged only in coastal trade, are required, occasionally, to serve ships arriving or departing on an international voyage.

III.2.1. The Government shall base its decision under section III.2 on a port facility security assessment carried out in accordance with the provisions of this Act.

III.2.2 Any decision which the Government makes, under section III.2 shall not compromise the level of security intended to be achieved by this Act.

III.3 This Act does not apply to warships, naval auxiliaries or other ships owned or operated by any other State, party to the International Convention for the Safety of Life at Sea 1974[13] as amended, and used only on non-commercial service.

III.4 This Act shall apply to all shipping companies, which operate in Cameroon.

III.5 This Act shall apply to all the port facilities and installations in Cameroon required to serve ships arriving or departing on an international voyage.

III.6 Nothing in this Act shall prejudice the rights or obligations of States under international law.

IV RESPONSIBILITIES OF THE GOVERNMENT

IV.1 Subject to the provisions of this Act, the Government of Cameroon shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include but are not limited to:

1. the degree that the threat information is credible;

2. the degree that the threat information is corroborated;

3. the degree that the threat information is specific, imminent; and

[13] Hereinafter referred to as the SOLAS (Convention).

4. the potential consequences of such a security incident.

IV.2 When setting security level 3, the Government shall issue, as necessary, appropriate instructions and shall provide security-related information to the ships and port facilities that may be affected.

IV.3 The Government may delegate to the police, gendarme or the military certain of the security-related duties under this Act with the exception of:

1. setting of the applicable security level;

2. approving a port facility security assessment and subsequent amendments to an approved assessment;

3. determining the port facilities which will be required to designate a port facility officer;

4. approving a port facility plan and subsequent amendments to an approved plan;

5. exercising control and compliance measures pursuant to the provisions of this Act;

6. establishing the requirement for a Declaration of Security.

IV.I Declaration of Security

IV-I.1 The Government 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.

IV-I.2 A ship can request completion of a Declaration of Security when:

1. the ship is operating at a security level higher than that of the port facility or another ship it is interfacing with;
2. there is an agreement on a Declaration of Security between States parties to the ISPS Code 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.

IV.I.3 Requests for the completion of a Declaration of Security, under this Act, shall be acknowledged by the applicable port facility or ship.

IV.I.4 The Declaration of Security shall be completed by:

1. the Master or the ship security officer on behalf of the ship(s); and, if appropriate,

2. the port facility security officer or, if the Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

IV.I.5 The Declaration of Security shall address the security requirements that could be shared by between a port facility and a ship (or between ships) and shall state the responsibility for each.

IV.I.6 The Government shall specify, bearing in mind the provisions of this Act, the minimum period for which Declarations of Security shall be kept by the port facilities located within the country and territorial waters.

IV.I.7 The Government shall, bearing in mind the provisions of this Act, specify the minimum period for which Declarations of Security shall be kept by ships entitled to fly the nation's flag.

IV.II Port Facility security

IV.II.1 A port facility is required to act upon the security levels set by the Government, Government agencies, or local government authority in charge of maritime security within the national territory and territorial waters. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship` s personnel and visitors, goods and services.
IV.II.2 At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the Guidance given in Part B of this Act, in order to identify and take preventive measures against security incidents:

1. ensuring the performance of all port facility security duties;

2. controlling access to the port facility;

3. monitoring of the port facility, including anchoring and berthing area(s);

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

5. supervising the handling of cargo;

6. supervising the handling of ship` s stores; and

7. ensuring that security communication is readily available.

IV.II.3 At security level 2, additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section IV.II.2 of this Act, taking into account the guidance given in Part B of this act.

IV.II.4 At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section IV.II.2 of this Act, taking into account the guidance given in Part B of this Act.

IV.II.4.i In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Government.

IV.II.5 When a port facility security officer is advised that a ship encounters difficulties in complying with the provisions of this Act, or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, following any security instructions given by the Government, the port facility security officer and the ship security officer shall liaise and co-ordinate appropriate actions.

IV.II.6 When a port facility security officer is advised that the ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

IV.II.I Port facility Security Assessment

IV.II.I.1 The port facility security assessment is an essential and integral part of the process of developing and updating the port facility security plan.

IV.II.I.2 The port facility security assessment shall be carried out by the Government. The Government may authorize the Police, Gendarme, or the Military, to carry out the port facility security assessment of a specific, or all the port facilities within the territory or territorial waters.

IV.II.I.2.1 When the port facility security assessment has been carried out by any of the bodies as designated in Section IV.III.2, the security assessment shall be reviewed and approved for compliance with this section of the Act by the Government.

IV.II.I.3 The body carrying out the security assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, taking into account the guidance given in Part B of this Act.

IV.II.I.4 The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats and minor changes in port facilities, and shall always be reviewed and updated when major changes to the port facilities take place.

IV.II.I.5 The port facility assessment shall include, but not be limited to the following elements:

1. identification and evaluation of important assets and infrastructure it is important to protect;

2. identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

3. identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and

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

IV.II.I.6 The Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment and design of these port facilities are similar. It will be the responsibility of the Government to communicate the particulars of such an arrangement to the IMO if it adopts such an approach.

IV.II.I.7 Upon completion of the port facility security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

IV.III Port Facility Security Plan

IV.III.1 A port facility security plan shall be developed and maintained, on the basis of a port facility security assessment for each port facility, adequate for the

ship/port interface. The plan shall make provisions for the three security levels, as defined in this Part of the Act.

IV.III.1.i Subject to the provisions of Section IV.IV.2, of this Act, the Police, Gendarme, or the Military, may assist the Port Authorities in preparing the port facility security plan of a specific port facility.

IV.III.2 The Government must approve the port facility security plan as elaborated by the designated authority in charge thereof.

IV.III.3 Such a plan shall be developed taking into account the guidance given in part B of this Act and shall be in the working language of the port facility. The working language for the purpose of communicating with all the vessels that call at the ports will be the English language. French and/or English can be used for internal administrative purposes The plan shall address, at least, the following:

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

2. measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restrict areas of the facility;

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

4. procedures for responding to any security instructions the Government will give at security level 3;

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

6. duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects

7. procedures for interfacing with ship security activities;
8. procedures for the periodic review of the plan and updating;

9. procedures for reporting security incidents;

10. identification of the port facility security officer, including 24-hour contact details;

11. measures to ensure the security of the information contained in the plan;

12. measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

13. procedures for auditing the port facility security plan;

14. procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

15. procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers` welfare and labour organizations.

IV.III.4 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 port facility.

IV.III.5 The port facility security plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans.

IV.III.6 The Government shall determine which changes to the port facility security plan shall not be implemented unless they approve the relevant amendments to the plan.

IV.III.7 The plan will be kept in hard copies and electronic format. In the latter case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

IV.III.8 The plan shall be protected from unauthorized access or disclosure.

IV.IV Port Facility Security Officer

IV.V.1 A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

IV.IV.2 In addition to those specified elsewhere in this Part of this Act, the duties and responsibilities of the port facility officer shall include, but are not limited to:

1. conducting an initial comprehensive security survey of the port facility, taking into account the relevant port facility security assessment;

2. ensuring the development and maintenance of the port facility security

plan;

3. implementing and exercising the port facility security plan;

4. undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;

5. recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;

6. enhancing security awareness and vigilance of the port facility personnel;

7. ensuring adequate training has been provided to personnel responsible for the security of the port facility;

8. reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;

9. co-ordinate implementation of the port facility security plan with the appropriate company and ship security officer(s);

10. co-ordinating with security services, as appropriate;

11. ensuring that standards for personnel responsible for security of the port facility are met;

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

13. assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

IV.IV.3 The port facility security officer shall be given the necessary support by the Government to fulfill the duties and responsibilities imposed by the ISPS Code and this Part of this Act.

IV.V Training, Drills and Exercises on Port Facility Security

IV.V.1 The port facility security officer and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in Part B of this Act.

IV.V.2 Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the port facility security

plan, and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part B of this Act.

IV.V.3 To ensure the effective implementation of the port facility security plan, drills shall be carried out at appropriate intervals, taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in part B of this Act.

IV.V.4 The port facility security officer shall ensure the effective co-ordination and implementation of the port facility security plan by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Act.

V Obligations of the Company

V.I The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or the Government as may be necessary.

V.II The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfill their duties and responsibilities in accordance with the provisions of the ISPS Code and this Part of this Act.

V.III The proper carrying out of these duties will be incumbent upon the Company` s acting upon the security level as determined by the Government and nominating security personnel with defined functions as provided in section V.V.4 of this Part of this Act.

V.IV It is the responsibility of the Government to ensure that all ships registered under its flag meet all the provisions of this Act and to issue certificates to attest to their compliance.

V.V The Government has to make sure, through the Officers in charge of port State control, that all ships intending to call to any of the ports in the country carry the necessary security certificates involving a detailed ship security plan.

V.V.1 Ship Security

V.V.1.1 A ship is required to act upon the security levels set by the Government as set out below.

V.V.1.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in Part B of this Act, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship security duties;

.2 controlling access to the ship;

.3 controlling the embarkation of persons and their belongings;

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

.5 monitoring of deck areas and areas surrounding the ship;

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

.7 ensuring the security communication is readily available.

V.V.1.3 At security level 2, additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section V.V.1.2, taking into account the guidance given in Part B of this Act.

V.V.4 At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section V.V.1.2 of this Act, taking into account the guidance given in Part B of this Act.

V.V.5 Whenever the Government sets security level 2 or 3, the ship shall acknowledge receipt of the instructions on change of the security level.

V.V.6 Prior to entering any of the ports of Cameroon, or whilst in any of the ports in Cameroon, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and the ship security officer shall liaise and co-ordinate the appropriate actions.

V.V.7 If a ship is required by the Government to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the Government, through the port facility security officer, of the situation.

V.V.7.i In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

V.V.8 When the Government sets security levels and ensures the provision of security-level information to ships operating in its territorial sea, or having communicated

an intention to enter its territorial sea, such ships shall be advised to maintain vigilance and report immediately to their flag administrations and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

V.V.8.i When advising such ships of the applicable security level, the Government shall, taking into account the guidance given in Part B of this Act, also advise those ships of any security measures that they should take and, if appropriate, of measures that have been taken by the Government to provide protection against the threat.

V.V.2 Ship Security Assessment

V.V.2.1 The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

V.V.2.2 The company security officer shall ensure that persons with appropriate skills evaluate the security of a ship, in accordance with this section, taking into account the guidance given in Part B of this Act.

V.V.2.3 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.

V.V.3 Ship Security Plan

V.V.3.1 Each ship shall carry on board a ship security plan approved by the flag State. The plan shall make provisions for the three security levels as defined in this Part of this Act.

V.V.3.1.1 Subject to the provisions of section V.V.3.2.1, the police, gendarme or the military, may assist in the preparation of the ship security plan for a specific ship.

V.V.3.2 The flag State may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations like the police, gendarme r the military.

V.V.3.2.1 In such cases, the recognized security organization undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

V.V.3.3 The submission of a ship security plan, or of amendments to a previously approved plan, for approval shall be accompanied by the security assessment of the basis of which the plan, or the amendments, has been developed.

V.V.3.4 Such a plan shall be developed, taking into consideration, the guidance provided in Part B this Act, and shall be written in the working language or languages of the ship. If the language or languages used is not English, French, or Spanish, a translation into one of these languages shall be included. The 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 or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions the Government 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 and updating of the plan;

.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.

V.V.3.5 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 nature of the company or of the ship.

V.V.3.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

V.V.3.7 The plan shall be protected from unauthorized access or disclosure.

V.V.4 Ship Security Officer

V.V.4.1 A ship security officer shall be designated on each ship by the Company.

V.V.4.2 In addition to those specified elsewhere in this part of the act, 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 security plan, including any amendments to the plan;

.3 co-ordinating 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 onboard;

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

.8 reporting all security incidents;

.9 co-ordinating 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.

V.V.5 Company security Officer

V.V.5.1 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 clear 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.

V.V.5.2 In addition to those specified elsewhere in this Part of the Act, the duties and responsibilities of the company security officer shall 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 the 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 Government, the Police, Gendarme or the Military;

.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 co-operation 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

V.V.6 Training, Drills and Exercises on Ship Security

V.V.6.1 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 this Act.

V.V.6.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in Part B of this Act.

V.V.6.3 Shipboard personnel having specific security duties and responsibilities 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 this Act.

V.V.6.4 To ensure the effective implementation of the ship security plan, 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, taking into account the guidance provided in Part B of this Act.

V.V.6.5 The company security officer shall ensure the effective co-ordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance provided in Part B of this Act.

V.V.7 Keeping of Records Concerning all Incidents Relating to Ship Security

V.V.7.1 The Government shall stipulate the minimum period for which records of all activities concerning the following shall be kept on board ships:

.1 training, drills and exercises;

.2 security threats and security incidents;

.3 breaches of security;

.4 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 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.

V.V.72 The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

V.V.7.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment.

V.V.7.4 The records shall be protected from unauthorized access or disclosure.

VI Co-operation and Co-ordination

VI.1 The Government shall ensure that there is a forum for the exchange of all information relating to maritime security between all the maritime operators in Cameroon. In so doing the Government has to ensure the following:

VI.2 The setting up of an office for the co-ordination of security of ships and of port facilities in, or around the ports.

VI.2.1 The Companies shall provide information on their security requirements, and the particulars of all their ships to this office prior to the arrival of all their ships and a record of the intended work to be done at the ports.

VI.2.2 All the information so provided by the Company must be corroborated by the ship master or ship security officer before the ship is piloted into port.

VI.3 Designate trained personnel who will be responsible on a 24-hour basis to make sure they monitor all the activities of ships that enter and leave the ports and take down record of their activities.

VI.4 The Government shall establish communication links with the ports of the neighboring countries and ensure that there is technical co-operation and co-ordination with respect to ship and port security.

VII Verification and Certification for Ships

VII.1 Verifications

V.II.1.1 Each ship to which this Part of the Act applies shall be subject to the verifications specified below:

.1 an initial verification before the ship is put in service or before the certificate required under section V.II.2 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of SOLAS, of this Act and of the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of SOLAS

and this part of this Act, is in satisfactory condition and fit for the service for which the ship is intended;

.2 a renewal verification at intervals specified by the Government, but not exceeding five years, except where section V.II.3 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 of SOLAS, this Part of the Act and the approved ship security plan, is in satisfactory condition and fit for the service for which the ship is intended;

.3 there should be at least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second third anniversary dates of the certificate as defined in the regulation I/2(n) of SOLAS. The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;

.4 The Government may determine any additional verifications.

VII.1.2 Government officials shall carry out the verification of ships. The Government may, however, entrust the verifications to the Police, Gendarme, or the Military, provided the responsible officials are familiar with ship and port facility security issues.

VII.1.3 In every case, the Government shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

VII.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-24.2 and XI-2/6, of this Part of the Act and of the approved ship security plan. After any verifications under section VII.1.1 has been completed, no changes shall be made in the security system and in any associated security equipment or the approved ship security plan without the authorization of the Government.

VII.2 Issue or Endorsement of Certificate

VII.2.1 An International Ship Security Certificate shall be issued after the initial renewal verification in accordance with the provisions of section V.II.1.

VII.2.2 Such certificate shall be issued or endorsed either by the Government or by recognized security organization acting on behalf of the Government.

VII.2.3 Another contracting Government may, at the request of the Government, cause the ship to be verified, and if satisfied that the provisions of section V.II.1 are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship, and where appropriate, endorse or authorize the endorsement of that certificate on the ship, in accordance with the Act.

VII.2.3.1 A copy of the Certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Government.

VII.2.3.2 A Certificate so issued shall contain a statement to the effect that it has been issued at the request of the Government and it shall have the same force and receive the same recognition as the Certificate issued under section V.II.2.2.

VII.2.4 The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix of the ISPS Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

VII.3 Duration and Validity of Certificates

VII.3.1 An international Ship Security Certificate shall be issued for a period specified by the Government, which shall not exceed five years.

VII.3.2 When the renewal verification is completed within three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

VII.3.2.1 When the renewal verification is completed after the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing Certificate.

VII.3.2.2 When the renewal verification is completed more than three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

VII.3.3 If a Certificate is issued for a period of less than five years, the Government may extend the validity of the Certificate beyond the expiry date to the maximum period specified in section V.II.3.1, provided that the verification referred to in section V.II.1.1 applicable when a Certificate is issued for a period of five years are carried out as appropriate.

VII.3.4 If a renewal verification has been completed and a new Certificate cannot be issued or placed on board the ship before the expiry date of the existing Certificate, the Government or recognized security organization acting on behalf of the Government may endorse the existing Certificate and such a Certificate shall be accepted as valid for a further period which shall not exceed five months from expiry date.

VII.3.5 If a ship, at the time when the Certificate expires, is in any of the ports in Cameroon, the Government may extend the period of validity of the Certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and then only in cases where it appears proper and reasonable to do so. No Certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new Certificate. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the expiry date of the existing Certificate before the extension was granted.

VII.3.7 If an intermediate verification is completed before the period specified in section V.II.1.1, then;

.1 the expiry date shown on the Certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;

.2 the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by section V.II.1.1 are not exceeded.

VII.3.8 A Certificate issued under section V.II.3.2 shall cease to be valid in any of the following cases:

.1 if the relevant verifications are not completed within the periods specified under section V.II.1.1;

.2 if the Certificate is not endorsed in accordance with section V.II.1.1.3 and V.II.3.9.1, if applicable;

.3 when a company assumes the responsibility for the operation of a ship not previously operated by that company; and

.4 upon transfer of the ship to the flag of another state.

VII.3.9 In the case of:

.1 a company that assumes responsibility for the operation of a ship not

previously operated by that company, the previous company shall, as soon as possible, transmit to the receiving company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in section V.II.3.2.

VII.4 Interim Certification

VII.4.1 The Certificates specified in section V.II.2 should be issued only when the Government is fully satisfied that the ship complies with the requirements of section VII.1. However, after 1 July 2004, for the purposes of:

.1 a ship without a Certificate, on delivery or prior to its entry or re-entry into service;

.2 transfer of a ship from the flag of one State to another;

.3 transfer of a ship from the flag of a State non-member to SOLAS, to a State
party to the SOLAS;

.4 a Company assuming the responsibility for the operation of a ship not previously operated by that Company;

until the Certificate referred to in section V.II.2 is issued, the Government may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the appendix of Part A of the ISPS Code.

VII.4.2 An Interim International Ship Security Certificate shall only be issued when the Government or recognized security organization acting on its behalf has verified that:

.1 the ship security assessment required by this Part of the Act has been completed;

.2 a copy of the ship security plan meeting the requirements of chapter XI-2 of SOLAS and this Part of the Act 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 regulation XI-2/6, if required;

.4 the company security officer:

.1 has ensured that:

.1 the review of the ship security plan for compliance with this Part of the Act;

.2 that the plan has been submitted for approval; and

.3 that the plan is being implemented on the ship; and

.2 has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the company security officer is satisfied that the ship will successfully complete the required verification in accordance with section V.II.1.1.1, within six months;

.5 arrangements have been made for carrying out the required verifications under section V.II.1.1.1;

.6 the master, the ship security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this part of the Act; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship`s personnel or languages understood by them; and

.7 the ship security officer meets the requirements of this Part of the Act.

VII.4.3 An Interim International Ship Security Certificate may be issued by the Government or by a recognized security organization authorized to act on its behalf.

VII.4.4 An Interim International Ship security certificate shall be valid for six months, or until the Certificate required by section V.II.2 is issued, whichever comes first, and may not be extended.

VII.4.5 The Government shall not cause a subsequent, consecutive Interim International Ship security Certificate to be issued to a ship if, in its judgment or that of the recognized security organization entitled to act on its behalf, one of the purposes of the ship or a company in requesting such Certificate is to avoid full compliance with chapter XI-2 of SOLAS and this Part of the Act beyond the period of the initial Interim International Ship Security Certificate as specified in section V.II.4.4.

VII.4.6 For the purposes of regulation XI-2/9 of SOLAS, the Government may, prior to accepting an Interim International Ship Security Certificate as a valid Certificate, ensure that the requirements of sections V.II.4.2.4 to V.II.4.2.6 have been met.

VIII Final Provisions

VIII.I The President of the Republic will append his signature to the final Act when voted by the Parliament and the Act will enter into force immediately thereafter.

VIII.II The Act shall be published in the official gazette and copies thereof provided to all Government Agencies, national and local, having a bona fide connection with maritime affairs.

VIII.III The Government reserves the right to amend any provision(s) in this Act at any time as it deems necessary and can require any foreign vessel owner or operator in Cameroon to strengthen its security measures as may be necessary in the particular circumstance.

Appendix to part A
Appendix 1
Form of the International Ship
Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(Official seal) **Cameroon**

Certificate Number …….....

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

under the authority of the Government of

Cameroon

_____
(Person or Organization authorized)

Name of ship…….

Distinctive number of letters……

Port of registry……..

Type of ship …….....……..

Gross tonnage ……...

IMO Number …….

Name and address of the Company……..

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 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 certificate)

Date of issue ……..

(Signature of the duly authorized official issuing the Certificate)

……

(Seal or stamp of issuing authority as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERTIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code at 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 the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERTIFICATIONS*

Additional verification **Signed: ……**
(Signature of authorized official)

Place: ……

Date: ……
(Seal or stamp of the authority, as appropriate)

Additional verification **Signed: ……**
(Signature of authorized official)

Place: ……

Date: ……
(Seal or stamp of the authority, as appropriate)

Additional verification **Signed: ……**
(Signature of authorized official)

Place: ……

Date: ……

(Seal or stamp of the authority, as appropriate)

ADDITIOINAL VERTIFICATION 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 Convention and part A of the ISPS Code.

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

(Seal or stamp of the 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, be accepted as valid until……

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT WHERE THE RENEWAL VERTIFICATION 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 190.3.3 of part A of the ISPS Code, be accepted as valid until……..

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

(Seal or stamp of the authority, as appropriate)

ENDORSEMENRT WHERE THE RENEWAL VERTIFICATION 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 190.3.3 of part A of the ISPS Code, be accepted as valid until……..

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

(Seal or stamp of the authority, as appropriate)

The government of Cameroon has established that the validity of this statement of compliance is subject to mandatory annual or unscheduled verifications.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code the port facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

1ST VERIFICATION

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

2nd VERIFICATION

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

3 rd VERIFICATION

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

4thVERIFICATION

Signed: ……
(Signature of authorized official)

Place: ……

Date: ……

Appendix 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) **Cameroon**

Certificate Number ……

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

under the authority of the Government of

Cameroon

(Person(s) or organization authorized)

Name of ship ……

Distinctive number or letters……..

Port of registry ……

Type of ship ……

Gross tonnage ……

IMO Number ……

Name and address of Company …….

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 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 Certificate)

Date of issue …… …….
(Signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority as appropriate)

PART B

GUIDELINES REGARDING THE APPLICATION OF PART A OF THIS ACT.

Contents

Appendices

Abbreviations

ILO	International Labour Organization
IMO	International Maritime Organization
ISPS Code	International ship and port facility security
PFSO	Port facility security officer
PFSP	Port facility security plan
PSA	Port security assessment
PSAC	Port security advisory committee
PSO	Port security officer
PSP	Port security plan
Pt	Potential target
SOLAS	International Convention for the Safety of Life at Sea, 1974, as amended
TRAM	Threat and risk analysis matrix

1. INTRODUCTION

1.1 The objective of these guidelines on security in ports and on ships is to enable the Government of Cameroon, employers. workers and other stakeholders to reduce the risk to ports and ships from the threat posed by unlawful acts. The guidelines provide a guidance framework to develop and implement a port and ship security strategy appropriate to identified threats to security.

1.2 The guidelines of security in ports and on ships are part of an integrated approach to ship and port-related security, safety and health issues where security fits into existing health and safety guidance documents.

1.3 These guidelines are intended to promote a common approach to ship and port security amongst all the maritime operators in Cameroon.

1.4 These guidelines are intended to be compatible with the provisions of SOLAS, the ISPS Code and resolutions adopted by the conference of Contracting Governments to the SOLAS Convention on the 9-13 of December 2002. Where terms used in these guidelines differ from those contained in the ISPS Code, they are specified.

1.5 These guidelines are not intended to replace the ISPS Code. They extend beyond the area of the particular port facility and ships, which attracts a security incident to the whole port..

1.6 The measures proposed within these guidelines will apply to the entire port, as defined in the ISPS Code. However they are not intended to replace the security measures in place within the port facility. The PSA and PSP should take into account the security measures in place within the port facilities paying attention to the relationship between each port facility and the rest of the port.

1.7 These guidelines provide a method of identifying potential weaknesses in a ship's security system and outlines security roles, tasks and measures to detect and respond to unlawful acts against ships and ports serving the international traffic and maritime operations by:

1.7.1 recommending that a security assessment is carried out by an appropriate authority in each port and on every ship by a designated security officer.

1.7.2 recommending that a port security advisory committee be formed.

1.7.3 recommending that a security plan be produced covering the issues identified in the assessment and identifying appropriate security measures to be implemented.

1.7.4 applying security guidelines to all areas and functions of the port and on the board ships and those working in, having business with and requiring access to the port or transiting through the port. This includes port workers and other port personnel, seafarers, passengers and passengers' baggage, cargo, material, and stores vehicles and equipment originating from within and outside the port area.

1.7.5 promoting security awareness in the port and on the ships and the training of personnel appropriate to their roles and responsibilities.

1.7.6 maximizing the effectiveness of security measures through systematic drills, exercises, tests and audits of security procedures to identify and correct non-compliance, failures and weakness.

1.8 The guidelines should be aligned with the Cameroon Government's security and safety strategies.

1.9 These guidelines do not effect obligations to comply with applicable national laws. Regulations and rules.

1.10 These guidelines do not make particular reference to the company, the ship, company security officer, ship security officer, ship security assessment and ship security plan. This is so because it is the role of the flag state to ensure compliance with the security measures and the government only controls through its port state control officers to ensure that foreign ships comply with the provisions of part AS of the ISPS code and Part A of this Act.

2. SCOPE AND DEFINITIONS

2.1 **SCOPE.** These guidelines, though not mandatory, should, when applicable, apply, as appropriate, to all persons organizations or entities operating in, transiting through or having any other legitimate reason to be in the port or on board the ship in any port in Cameroon.

2.2 **DEFINITIONS** used in this part of the guidelines are to the extent practicable in keeping with those contained in the international convention for he safety if life at sea (SOLAS) 1974., as amended. For ease of reference certain terms used in these guidelines are defined in this section.

2.3 **PORT.** For the purposes of these guidelines port means the geographic area defined by the Government or the designated authority (including port facilities as defined in the International Ship and Port Facility Security (ISPS) Code), in which maritime and other activities occur.

2.4 **THE GOVERNMENT.** As defined in section II.2 of Part A of this Act.

2.5 **DESIGNATED AUTHORITY**. The Governmental Organization(s) or the authority (ies) identified within the government, responsible for the security of ports.

2.6 **SECURITY.** A condition where the level of risk is deemed acceptable.

2.7 **THREAT.** The likelihood that an unlawful act will be committed against a particular target, based on a perpetrator's intent and capability

2.8 **SECURITY INCIDENT**. Any act or circumstance affecting the security of a ort or a ship.

2.9 **SECURITY Level.** The qualification of the degree of risk that a security incident will be attempted or will occur.

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

2.9.2 **Security level 2**- the security 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.

2.9.3 **Security level 3** – The security level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probably or imminent although it may not be possible to identify the specific target.

2.10 **PORT SECURITY OFFICER (PSO)** The person or persons tasked to manage and coordinate security in the port.

2.11 **PORT SECURITY ADVISORY COMMITTEE (PSAC)** A committee established by the member State of the designated authority responsible, inter alia, to act as a security consultative body and to be involved in the continuous development and implementation of the port security plan.

2.12 **PORT SECURITY ASSESSMENT (PSA).** A comprehensive evaluation by the member State or the designated authority of threats, vulnerabilities, capabilities, preparedness and existing security measures related to the port, forming an essential and integral part of the process of developing a port security plan.

2.13 **PORT SECURITY PLAN (PSP).** A Written document that describes the measures the member State or the designated authority and members of the port community should take to reduce vulnerabilities, deter threats and respond to security incidents. |It should address issues impacting upon the security of the port and , where applicable may take into account issues relating to any port facility security plan or other security plan.

2.14 **SHIP SECURITY OFFICER (SSO).** The person or persons tasked to manage and coordinate security on board the ship,

2.15 **SHIP SECURITY ASSESSMENT (SSA).** A comprehensive evaluation by the Government or the designated authority of threats, vulnerabilities, capabilities, preparedness and existing security measures related to a ship, forming an essential and integral part of the process of developing a ship security plan.

2.16 **SHIP SECURITY PLAN (SSP).** A written document that describes the measures the Government of the designated authority and national maritime community should take to reduce vulnerabilities, deter threats and respond issues impacting upon the security of ship.

2.17 **PORT FACILITY.** A location as determined by the Government or by the designated authority where the ship/port interface as described in the ISPS Code takes place.

2.18 **INFRASTRUCTURE.** Is used in its broader meaning, which includes superstructures, services and other installations.

2.19 **SECURITY SENSITIVE INFORMATION.** Information, the disclosure of which would compromise the security of the port, including but not limited to, information contained in any personnel-related file or privileged or confidential information that would compromise any person or organization.

3. AIM OF SECURITY MEASURES

3.1 The aim of port and ship security measures is to maintain an acceptable level of risk at all security levels.

3.2 Security measures should be devised to reduce risks and should in the main revolve around procedures to establish and control access to restricted areas and other venerable or sensitive key points, functions or operations in the airport and on board ships.

3.3 Some examples of the aim of security measures that may be considered are to:

3.3.1 Prevent access to the port by persons without a legitimate reason to be there and prevent those persons with legitimate reasons to be in the port from gaining illegal access to ships or other restricted port areas for the purpose of committing unlawful acts.

3.3.2 Prevent introduction of unauthorized weapons, dangerous or hazardous substances and devices, into the port or vessels using the port.

3.3.3 Prevent personal injury or death, or damage to the port, port facility , ship or port infrastructure by explosive or other devices.

3.3.4 Prevent tampering with cargo, essential equipment, containers, utilities protection systems, procedures and communication systems affecting the port and ships.

3.3.5 Prevent smuggling of contraband, drugs, narcotics, other illegal substances and prohibited material.

3.3.6 Prevent other criminal activities, such as theft.

3.3.7 Protect against the unauthorized disclosure of classified material commercially proprietary information on security sensitive information.

4. Security policy

4.1 The Government should produce a "ports security policy statement" that provides the foundation to develop directives, rules and regulations as appropriate. Port security policies should take into account relevant international conventions, codes, these guidelines and other established national practices. The policy should consider ships registered under the national flag as well as ships that call at the country's ports.

4.2 The government should develop a security policy and ensure a legal framework is in place to carry out the provision of these guidelines. The security policy should address the government's measures to:

4.2.1 Promote regional and international cooperation;
4.2.2 Encourage maximum stakeholder participation in policy development;
4.2.3 Provide adequate resources of the human element: safety and security awareness, training and skill development;
4.2.4 Recognize the interdependence between security and public safety, economic development and protection of the environment;
4.3 The security policy should be periodically reviewed and update to reflect changing circumstances.

5. Roles and tasks

5.1 **The government**. In addition to the development of a security policy, the government should:

5.1.1. Identify the designated authority for each port required having a port security

plan;

5.1.2. Ensure the establishment of a port security advisory committee and the

nomination of a port security officer;

5. 1.3. Nominate the persons responsible for port security operations in a specific

port, in accordance with the provisions of part A of this Act;

5.1.4. Ensure that a port security assessment is carried out;

5. 1.5. Approve port security assessments and any subsequent amendments thereto;

5. 1.6. Ensure that port security plans are properly developed, implemented and

periodically reviewed and maintained;

5. 1.7. Set and communicate the appropriate security level. it carried out. The government may delegate any of the functions referred to in 5. 1.2 through 5. 1 .6 above to the designated authority.

5.1.8 Ensure that there is a special department in-charge of the translation and interpretation of foreign ships' security certificates into English, French or Spanish and to ensure adequate communication and Understanding.

5.1.9 Set a program of communication and collaboration with neighboring countries in matters relating to maritime security and the training of security personnel through the regional co-operation.

5.2. **Port Security Officer (PSO).** Tasks of the PSO should include, inter alia. the following:

5.2. 1. Conducting an initial comprehensive security survey of the port. taking into account the relevant port security assessment.

5.2.2. Ensuring the development and maintenance of the port security plan.

5.2.3. Implementing the port security plan.

5.2.4. Undertaking regular security inspections of the port to ensure the continuation of appropriate measures.

5.2.5. Recommending and incorporating, as appropriate, modifications to the port security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port.

5.2.6. Enhancing security awareness and vigilance of the port's personnel.

5.2.7. Ensuring that adequate training has been provided to personnel responsible for the security of the port.

5.2.8. Reporting to the relevant authorities and maintaining records of security incidents that affect the security of the port.

5.2.9. Coordinating implementation of the port security plan with the appropriate persons or organizations.

5.2.10. Coordinating with security services, as appropriate.

5.2.11. Ensuring that standards for personnel responsible for security of the port are met.

5.2.12. Ensuing that security equipment is properly operated. tested. calibrated and maintained.

5.3. Port Security Advisory Committee (PSAC). A PSAC should be established for every port. Where applicable, with full terms of reference, the PSAC should act as a consultative and advisory body with a designated chairperson. The PSAC should cooperate with applicable safety and health committees, as appropriate. The PSAC's role should be to (as appropriate but not limited to):

5.3.1. Advise on the implementation of the port security plan and assist iii conducting the port security assessment.

5.3.2. Coordinate, communicate and facilitate implementation of the applicable security measures required by the port security plan.

5.3.3. Provide feedback on the implementation. drills and exercises. testing. Security training and periodic updates of the port security plan.

5.3.4. Ensure its membership reflects the operational functions of the port and includes, as appropriate:

5.3.4.1. The PSO and PFSO(s).

5.3.4.2. National and local government border control authorities and security agencies.

5.3.4.3. Police, Gendarme, Military and Emergency Services.

5.3.4.4. Workers' representatives.[14]

5.3.4.5. Ship operator representatives.

5.3.4.6. Representatives of commercial concerns and tenants.

5.3.4.7. Trade associations.

5.3.4.8. Other relevant parties.

6. Security level

6.1. The appropriate security level is determined by the government. The security measures to be adopted appropriate to the security level should be outlined in the port security plan.

6.2. Changes in the security level should be quickly communicated to those with a need to know in response to a perceived or actual change in threat information.

6.3. In the event of a change in security level, the PSO should act in accordance with the PSP, and verify that the requirements of the PSP and any additional or special security procedures appropriate to the particular threat are applied. For example:

6.3.1. **Security level 1** measures may include random personnel, baggage. Materials, stores and vehicle screening, and implementation of access and movement control.

6.3.2. **Security level 2** measures may include increased frequency of screening. more robust monitoring of the port, and more stringent access and movement control measures.

6.3.3. **Security level 3** measures may include 100 per cent screening. Increased identification checks. Temporary cessation of certain port activities and/or imposing

[14] Throughout this text, when the term "workers' representatives" is used, it refers to Article 3 of the Workers' Representatives Convention, 1971 (No. 135), which reads as follows:

> For the purpose of this Convention the term " representative" means persons who are recognized as such under national law or practice, whether they are: (a) trade union representatives, namely, representatives designated or elected by trade unions or by the members of such unions; or (b) elected representatives, namely, representatives who are freely elected by the workers of the undertaking in accordance with provisions of national laws or regulations or of collective agreements and whose functions do not include activities which are recognized as the exclusive prerogative of trade unions in the country concerned.

vessel traffic control measures, restricting access to certain areas, deployment of security personnel to key infrastructure. Etc.

7. Port Security Assessment (PSA)

7. 1. The port security assessment should be carried out by persons with the

appropriate skills and should include the following:

7.1.1. Identification and evaluation of critical assets and infrastructure that it is

important to protect.

7. 1.2. Identification of threats to assets and infrastructure in order to establish and prioritize security measures.

7.1.3. Identification, selection and prioritization of measures and procedural changes and their level of acceptance in reducing vulnerability.

7.1.4. Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

7.1.5. Identification of perimeter protection, access control and personnel clearance requirements for access to restricted areas of the port.

7.1.6. Identification of the port perimeter and. where appropriate, the identification of measures to control access to the port at various security levels.

7. 1.7. Identification of the nature of the expected traffic into or out of the port (e.g. passengers, crew, ship/cargo type).

7.2. One example of a method and risk-based tool to assist in preparing a port security assessment is included in Appendix A. Other tools may be used.

8. Port Security Plan (PSP)

8.1 The port security plan should be based on the PSA and include:

8.1.1. Details of the security organization of the port.

8. 1.2. Details of the port's links with other relevant authorities and the necessary communications systems to allow the effective continuous operation of the organization and its links with others.

8.1.3. Details of security level 1 measures, both operational and physical, that will be in place.

8.1.4. Details of the additional security measures that will allow the port to progress without delay to security level 2 and, when necessary, to security level 3.

8. 1.5. Provision for the regular review, or audit of the PSP and for its amendment in response to experience or changing circumstances.

8.1.6. Details of the reporting procedures to the appropriate member States' contact points.

8.1.7. Details of the necessary liaison and coordination between the PSO and any PFSOs.

8.1.8. Identification of restricted areas and measures to protect them at different

security levels.

8.1.9. Procedures for the verification of identity documents.

8. 1.10. Requirements for drills and exercises carried out at appropriate intenrals to ensure the effective implementation of the PSP.

8.2. The PSP should refer to, and t into account, any other e port emergency plan or other security plans.

8.3. The PSP should be protected from unauthorized access or disclosure.

8.4. One example layout and content of a port security plan is included in Appendix .

9. Physical security of the port

9.1. At each security level the PSP should identify the location of restricted areas, key points, vulnerable areas and critical functions in or associated with the port and the physical protection and access control procedures and access documents required to reduce the level of risk.

9.2. Areas designated as 'restricted areas" in the PSP should be delineated as such with appropriate warning signs, markings and as appropriate to the security level in force, barriers and access control points. The use of 24/7 CCTV should be installed.

9.3. Access control procedures should be established for restricted areas of the port for any person, vehicle, vessel, cargo, material, equipment and stores inbound or outbound whether from adjacent property, waterway or from outside the port.

9.4. The PSP should define the procedures for:

9.4.1. The issuance, verification and return of access documents, at no cost to the workers.

9.4.2. The details of verification to be made regarding those persons required to be provided with or issued, access documents.

9.4.3. The appropriate authorized access control requirements for each restricted area and level of access.

9.4.4. The reporting of lost. missing or stolen documents.

9.4.5. Dealing with the misuse of access documents.

These procedures should also cover temporary personnel, contractors and visitors at each security level.

The seafarers' identification document, issued in accordance with the Seafarers' Identity Documents Convention (Revised). 2003 (No.. I S5). would meet all requirements of these guidelines for the purposes of identification and access.

9.5. Where it is necessary to combine security aspects of the PSP and the PFSP, then these should be clearly identified in the PSP. These procedures should ensure that the security requirements are compliant with national and international customs and export regulations.

10. Security awareness and training

10.1 Security awareness is vital to the safety, security and health of port personnel and others having a place of work in the port, who should be made aware of their responsibilities to fellow workers, the port community and the environment. Appropriate training of personnel working in the port should maximize personal awareness of suspicious behavior, incidents, events or objects when going about their daily tasks and the invaluable contribution to be made to the security of the port and its personnel by each individual. Included should be clear lines for reporting such matters to supervisors, managers or appropriate authorities. Additional or special training may be required for people in particular roles.

10.2. Training may be focused oil particular roles and tasks in the port or at external facilities serving the port such as:

10.2.1. Security and law enforcement personnel.

10.2.2. Stevedores and all those handling, storing and transporting or coming into contact with passengers. freight. cargo. material and stores or ships.

10.2.3. Other associated roles and tasks where personnel do not come into direct contact with passengers, freight. cargo. material and stores or ships as a matter of course but who are in administrative and support roles in the port or at associated facilities.

10.3. Consideration should also be given to circumstances where it would be ineffective or contrary to good security practice to train or give additional information to those without a direct need to know.

11. Confidentiality and non-disclosure of information

Contracts of employment or organizational rules should contain provisions requiring personnel not to divulge security-related information on tile port. security training, access control systems, locations of security or communications equipment and routines or business of the port to persons who do not have a direct need to know.

Appendix to Part B

Appendix 1

The port security assessment (PSA)

Introduction

1. The " Threat and Risk Analysis Matrix" (TRAM) is a simplified risk-bused method and tool to assist in carrying out a PSA. It is but one of a number of tools and is given here by way of example.

2. Its purpose is to identify threats with a view to initiating and recommending countermeasures to deter, detect and reduce the consequence of any potential incident should it occur, Such an analysis may be a valuable aid to allocating resources, forward planning, contingency planning and budgeting.

3. The TRAM should he updated as often as changing circumstances may dictate to maintain its effectiveness, This task would, normally, fall under the remit of the designated authority who should establish and maintain close links with security corps and key commercial and industrial service partners and customers.

4. In addition to the more obvious threats, the list of potential targets should be as comprehensive as possible with due regard to the function(s) of the port, legal, political, social, geographic and economic environment of the Country and the security environment specific to the port.

Assessment process

5. Table 1 is a blank version of' the TRAM. The object is to compare/evaluate security

measures that will reduce, independently, the vulnerability or impact and collectively reduce the

overall risk score, It should he borne m mind that introducing a security measure !br one threat may increase the risk of another,

6. **Potential targets (PT).** There should he a separate table for each potential target.) Identify PT through assessment of functions and operations, vulnerable areas, key points or persons in the port and in the immediate environs that may, if subject to an unlawful act, detrimentally impact on he security, safety of personnel or function of the port.

6.1. Establish "ownership of the identified PT. For Example:

6. 1.1. directly owned and controlled by the port operator or Government

6.1.2. directly owned by the port operator or government but rented, leased, occupied and controlled by other parties

6.1.3. owned, controlled and operated by other parties:

6.1.3.1. represented on the PSAC:

6. 1.3.2. not represented on the PSAC (consider whether membership would be appropriate

and/or beneficial to the port community).

7. Establish if there are any existing security measures, such as a perimeter fence, access control and/or security patrol or monitoring of the P If so, are they effective, can improvements be made?

8. **Threat scenario** (columns A and B of table 1). Consider threat scenarios from both internal and external sources to which the identified PT may Be vulnerable (input from police, security and intelligence services is essential).

8. 1 . Threat scenarios (amongst many) that it may he appropriate to consider:

8. 1.1 . direct attack to cause injury and loss of life or destroy functions and infrastructure of the port. To take over vehicles/vessels as means to inflict damage by ramming. Release of noxious or hazardous material either from vehicles/vessels or storage areas and so on:

8.1.2. sabotage:

8.1.2 kidnap and ransom (for reward, extortion or coercion).

9. Threat (column C of table 1). The probability of an incident occurring should be assessed on the following scale:

3 = High;

2 = Medium:

1 = Low.

The allocation of a particular threat score may be based on specific information received or the known characteristics of the potential target.

10. Vulnerability (column D of table 1). The vulnerability of the PT to each threat may he assessed as follows:

4 = No existing security measures/existing security measures are not effective (e.g. unrestricted access to target, target not monitored: personnel untrained: target easily damaged):

3 = Minimal security measures (e.g. restricted areas not clearly identified: inadequate access control procedures: sporadic monitoring: normal security training program; target susceptible to certain types of damage):

2 = Satisfactory security measures (e.g. restricted areas clearly identified and access is controlled: Formal security training program: adequate monitoring and threat awareness: target not easily damaged):

1 = Fully effective security measures (e.g. all of “2” plus, capable of promptly scaling to higher security level as needed: target difficult to damage or has sufficient redundancy to prevent disruption it’ certain functions are damaged).

11. **Impact.** Assess the impact (consequence) of each potential incident on the PT and port should it occur. Specific impacts" and priorities for a particular port may be substituted by the designated authority to meet the national security profile and requirements.

5 = Detrimental to security and safety (likely to cause loss of life, serious injuries and/or create widespread danger to public health and safety)

4 = Detrimental to public safety and/or national prestige (likely to cause significant environmental damage and/or localized public health and safety),

3 = Detrimental to the environment and/or economic function of the port (likely to cause sustained port-wide disruption and/or significant economic loss and/or damage to national prestige).

2 = Detrimental to assets, infrastructure, utility and cargo security (likely to cause limited disruption to an individual asset, infrastructure or organization).

l.= Detrimental to customer/port community confidence.

12. **Risk score**. Score is the product of threat x vulnerability x impact.

12.1. The highest score scenario will be:

Threat — High ……..	3
Vulnerability — No existing countermeasure ……	4
Impact — Potential loss of life/injury …….	5
Risk score …….	60

12.2. The lowest score scenario will be:

Threat — Low……	1
Vulnerability — Fully compliant…….……...	1
Impact — Little……...…….	1
Risk score…….……..	1

13. Action priority (column (1 of table I). Tabulating and listing the scores for each threat against each P1 will assist in assessing the priority in which to deal with each potential incident. The process should lead to indications of actions required to deter, detect and mitigate the consequences of potential incidents, resources available or required and appropriate security measures.

14 In assessing likely scenarios the history and modus operandi of illegal groups most likely to operate in the area should be considered when identifying The PT and determining and assessing the most appropriate security measures.

15. This is an assessed reduction of the score breach scenario based on the perceived effectiveness of the security measures when they have been put into effect. [result should give some guidance as to which actions and resources will have the greatest benefit in deterring attack of the PT. It may also indicate that some targets or threats do not need to he considered or that the security measure is not achievable because of resource or other constraints.

16. The TRAM for every potential target should he collated into one master matrix of similar threat scenarios and common security measures identified to give the maximum benefit. It may also be that some P1' may be grouped together under one security measure. For example one or more PT close together may he contained within one pen meter fence with one gate controller It may he that a vulnerable operation iii a remote part of the port Gail he moved into a more secure area. Every possible realistic action should he considered.

17. The completed TRAM together with a consolidated summary of all security measures that have heel) devised and are able to he implemented should form the basis from which the port security plan can he developed.

Assessment example

The following ten-step example is used to illustrate the possible working of a security assessment using the TRAM for a specific threat scenario — destroy port authority's communication tower by explosives.

Table 1. Blank Threat and Risk Analysis Matrix (TRAM)

Potential target: Person/place/location (identify each PT in the port area not covered by the PFSP or other official subordinate plan)

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1						
2						
3						
4						
5						
6						
7						
8						
9						

Step 1 – List feasible scenario in column B

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives					

Feasibility scenario as determined by current port security assessment

The tower is a critical component of port operational and commercial communications. It supports booster stations for local police and emergency service communications and, in addition, the tower supports mobile telephone repeater services for the area. Currently the tower is protected from casual access or interference by a 2-metre high razor wire fence of 15 metre diameter and is located in a non-restricted area approximately 200 metres from the Harbour Masters Office. The facility is positioned on flat ground approachable from all sides, and a service road, that is accessible from the public area roads, passes within 20 metres of the perimeter fence. Access to the compound is limited to maintenance and servicing of the tower components as required and seasonal ground maintenance including grass cutting by regular port approved contractors. There is a mobile security patrol that visits and checks for signs of damage or intrusion once by day and once by night. The tower could be easily damaged by an explosive device thrown over the fence, placed against the fence or a car bomb driven up to the compound or placed on the service approach road.

Step 2 – Assign a threat score to this scenario in column C

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1				

Threat score based on intelligence, security level, current deterrent measures and other relevant factors

This scenario has been given a threat score of "1-low" because no specific intelligence has been obtained that suggests communications facilities are being targeted at the present time. A score of "2-medium" or "3-high" may be given based upon intelligence.

Step 3 – Assign a vulnerability score to this scenario in column D

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1	2			

Vulnerability is the susceptibility of a potential target to a particular threat

In this example, the threat is damage to the communications tower by explosives. Vulnerability is listed as "2-satisfactory security measures" because the facility's existing perimeter fence and security patrol is considered a sufficient deterrent.

Step 4 – Assign impact score to this scenario in column E

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1	2	3		

Impact is the consequence of an incident – the effect on public health, safety or security, etc.

In this example, impact is listed as "3-detrimental to the economic function of the port" because there is no back-up communication tower, so its loss would shut down the port for some time until repairs could be made, thus causing substantial economic loss. Impact may be further reduced if there is redundancy to the potential target (e.g. a back-up communications tower) or if a target may be easily repaired. Conversely, impact may increase if there is no redundancy, or if a target would be difficult to replace.

Step 5 – Calculate the initial Risk score in column F

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1	2	3	6	

The initial score is calculated by multiplying columns C, D and E)

In this example the initial score would be "6" (1 x 2 x 3 = 6).

Step 6 – Determine the action priority in column G (typically performed following several scenario calculations)

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1	2	3	6	

The action priority is based on each scenario's initial score

Establishing action priorities based on initial Risk scores is a quick way to distinguish between the various scenarios, and can help focus and allocate scarce resources, particularly when a large number of scenarios are assessed.

Step 7 – Determine new scores and action priorities based on changes to threat, vulnerability or impact

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	2	2	3	12	

A variety of factors may change an initial risk score

For example, an increase in threat from 1 (low) to 2 (medium), would raise the risk score from "6" to "12" (column C increases from "1" to "2", thus 2 x 2 x 3 = 12; see above). When the threat score increases, persons involved in developing security measures can use this table to recalculate how vulnerability or impact reduction measures may reduce the risk score. If "6" is deemed to be an acceptable level, then vulnerability reduction measures or impact reduction measures should be considered that will reduce the figures in columns D and E so as to give a risk score in column F of no higher than "6".

Step 8 – Implementing measures to reduce vulnerability

As described in Step 1, the tower is protected from casual access or interference by a 2-metre high razor wire fence of 15 metre diameter and is located in a non-restricted area approximately 200 metres from the Harbour Master's Office. The facility is positioned on flat ground approachable from all sides, and a service road, that is accessible from the public area roads, passes within 20 metres of the perimeter fence. Access to the compound is limited to maintenance and servicing of the tower components as required and seasonal ground maintenance including grass cutting by regular port approved contractors. There is a mobile security patrol that visits and checks for signs of damage or intrusion once by day and once by night. With these measures, vulnerability was scored as "2". However, if additional vulnerability reduction measures, such as a full-time on-site security force, or, changing the non-restricted area to a restricted area, the vulnerability score may be reduced from "2" to "1" fully effective security measures. Thus, with vulnerability in column D reduced from "2" to "1", as shown below, a new risk score of "6" is produced.

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	2	1	3	6	

Step 9 – Implementing measures to reduce impact

Reducing the impact will alter the figure in column E and reduce the overall risk score. Recall that the tower is a critical component of port operational and commercial communications. It also supports booster stations for local police and emergency service communications. In addition the mast supports mobile telephone repeater services for the area. Assuming that there is no back-up communications tower, the impact of losing this tower was initially calculated as "3" in column E. However, if a back-up facility was available, it would create some redundancy, thereby reducing the impact of a loss. Thus, with impact reduced from "3" to "2" limited disruption to port organization due to communications redundancy, as shown below, produces a new risk score of "8". While this is an improvement from "12", the persons responsible for port security could then decide whether additional measures were needed.

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	2	2	2	8	

Step 10 – Implementing measures to reduce vulnerability and impact

If both the vulnerability reduction measures and impact reduction measures discussed in this example were taken together, the total risk score would be reduced to "4", well below the initial score of "6".

Scenario No.	Threat scenario	Threat	Vulnerability	Impact	Risk score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	2	1	2	4	

The persons doing the security assessment and persons charged with implementing security measures must determine the effectiveness of various vulnerability or impact reduction measures for their ports.

4.5. The form of the physical interface with the port facility (facilities) and movement of persons, material, stores and cargo between port facilities.

4.6. Safe and secure routes to, and area for holding suspect explosive devices and other suspicious objects.

Roles and tasks

5. The designated authority should require that all ports devise a PSP and nominate a PSO who along with the PSAC should implement the plan.

Format and content of the PSP

6. By way of example the following is given to assist the production of the PSP that may be made up of or contain the following information.

7. **Front/header page**
   Name of port area
   List of associated plans
   List of members of port security advisory committee
   Name, appointment and signature f person approving the plan
   Date of approval
   Authority for issue
   Date of issue

8. Distribution list — for unclassified and classified parts of the plan.

9. Record of changes — explanation of change procedures and tasks of plan holders to amend the plan and implement changes.

10. Table of contents — appendices may he used to segregate classified or commercially sensitive information and only distributed to those members of the port community approved to
receive the information.

11. Introduction. An explanation of the background, circumstances and objective of the port security plan. Include major objectives and security policies, e.g. to deter detect and respond through promotion of a high level of security awareness and training.

12. **Security policy statement**. Include a statement of the port security policy.

13. **Assumptions,** e.g.:

13.1.That unlawful acts may occur at any time with little or no warning.

13.2. Protection of human life, health and security is the most important consideration in development of the plan.

13.3. Maintaining the free flow of commerce and function of the port is a critical consideration.

13.4. That no single entity can provide all the resources required to provide adequate security measures and response to the consequences of an unlawful act.

13.5. That other disaster and contingency plans (e.g. dangerous goods, hazardous material or natural disaster response) will he activated as appropriate in response to any security incident.

13.6. That all members of the port community will voluntarily support and participate in measures to secure the port and its functions.

14. **Port security advisory committee** charter if applicable or authority for formation and:

14.1. Brief of role and task of the PSAC, e.g.:

14.1.1. To consult and advise on the implementation of the PSP and other security matters as appropriate.

14. 1.2 Develop procedures for sharing and communication of security-related information.

14. 1.3 Promote security awareness as the deterrent to unlawful acts.

15. **Organization and membership of the PSAC.** Make up of members of the PSAC and the relationship with other port and national or local planning committees.

16. **The Port.** Define the geographical and functional perimeter [boundaries] and make up of the port including all waterways and modes of transport, infrastructure and port and commercial functions.

17. Include associated infrastructure, facilities, functions and secondary ports to which a security threat may relate and that may be included in the main plan or other security plans.

18. List local law enforcement agencies and municipal emergency and support services (include local hospital/medical facilities) that may contribute to response and consequence management.

19. **Maps and charts**. Provide maps and charts showing all salient features and location of operations, functions and routes and access points including appropriate navigation channels. This may be attached as an annex to the plan.

20. **Operations and functions.** Detail maritime and non-maritime operations and functions.

21.**Critical operations and activities**. Identify and describe all critical operations and other significant activities carried out in the port area.

22 **Security levels.**

22.1 **Security level 1**. The level for which minimum appropriate protective security measures shall he maintained at all times.

22.2 **Security level 2.** The level for which appropriate additional protective security measures shall he maintained for a period of time as a result of heightened risk of a security incident.

22.3 **Security level 3.** The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent although it may not he possible to identify the specific target.

23 **Communications** Describe and detail the means of communicating security level(s) changes to the security level and methods of raising alarm in the event of an incident making sure that the language used is understood by all workers or make provision for translations thereof.

24. **Security measures, procedures and operations**. Tabulate and list in detail all security measures and operations that are to be implemented in the port at each security level in response to issues identified in the security assessment.

25. This should cover personnel security, perimeter and physical barriers, access control, CCTV surveillance and all approved security measures. It should detail the roles and tasks of all members of the port community to establish monitor/control, as appropriate, restricted areas and navigation zones.

26. It may he appropriate to use existing procedures to aid communication, implementation and testing. Where appropriate functional operating procedures and working instructions are in existence it may he feasible to add security elements to such procedures and working instructions. For example if there is an existing written operational procedure for checking contents of inbound vehicles against other documentation or information it may he possible to include security inspection of the contents in the existing procedure.

Roles, resources, authorities and tasks

27. Detail how and by whom security procedures will he implemented.

Relationship to other plans and organizations

28. List all other plans and organizations that may contribute to, relate to or impact on the PSS

Response and crisis management

29. Identify and list agencies and contacts responsible for responding, to mitigate the cause or consequence of an incident. Devise, tabulate and communicate a response plan for every perceived incident.

PSP review and maintenance policy

30. Define the policy and procedures to review and maintain the PSP.

PSP security and control

31. Define the distribution, dissemination and security of the plan, or parts of the plan, to achieve widest communication of its requirements without compromising security or proprietary information.

Training

32. Detail training requirements for port personnel to fulfill their role and that of their organization in carrying out tasks under the PSP.

Drills, exercises and testing

33. Methods should he detailed to carry out drills and exercises and to test the plan periodically, to check that it remains current and achievable by identifying changes that may impact on any critical response, resource or consequence factor.

Appendix to Part B
Appendix 2
Form of a Declaration of Security
between a ship and a port facility

DECLARATION OF SECURITY

Name of ship:	
Port of registry:	
IMO Number:	
Name of port facility:	

This Declaration of Security is valid from …… until ……. For the following activities: Cargo loading and unloading, passenger movement, ship repairs and all other services related to ship and cargo handling in the ports.

Under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

the port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of part A of the international code for the security of ships and of port facilities

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done in accordance with the relative approved plan, by	
Activity	The port facility :	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facilities, including berthing areas and areas surrounding the ship.		
Monitoring the ship, including berthing areas and areas surrounding the ship.		
Handling of cargo		
Delivery of ship’s stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Eensuring that security communication is readily available between the ship and the port facility		

The signatories of this agreement certify that security measures and arrangements for both the port facility part A of the code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at ……..…..…..... on the ……..…..……..…….

Signed for and behalf of	
The port facility:	The ship:
(signature of port facility security officer)	(signature of master or ship security officer)

Name and title of person who signed	
Name:	Name:
Title:	Title:

Contact details (to be completed as appropriate) (indicate the telephone numbers or the radio channels or frequencies to be used)	
For the port facility:	For the ship:
Port facility	Master
Port facility security officer	Ship security officer
	Company
	Company security officer

Appendix 3

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

(Official seal) Cameroon

Statement Number ……

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

The Government of

Cameroon

Name of port facility . . . . . .
Address of the port facility . . . . . .

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved port facility security plan. This plan has been approved for the following:

Passenger ship
Passenger high-speed craft
Cargo high-speed craft
Bulk carrier
Oil tanker
Chemical tanker
Gas carrier
Mobile offshore drilling units
Cargo ships other than those referred to above

This Statement of Compliance is valid until ……. Subject to verifications (as indicated overleaf)

Issued at ……
(place of issue of the statement)

Date of issue …… ……
(Signature of the duly authorized official
issuing the document)

(Seal or stamp of the issuing authority, as appropriate)

Appendix 4
References

The information given in this appendix is intended to provide background and references on guidelines and other sources of information that may be of interest.

1. Details of the following may be found on the IMO web site www.imo.org

1.1 International Convention for the Safety of Life at Sea, 1974 (SOLAS) (as amended).

1.2. International Ship and Port Facility Security Code (ISPS Code).

2. Seafarers' Identity Documents Convention (Revised). 2003 (No. 185) (available on the ILO website – www.ilo.org)

3. Information used in this guidelines is also sourced from web -site: www.un.org/docs

3. 1. United Nations resolution 57-219 — Protection of human rights and fundamental freedoms while countering terrorism.

3.2. United Nations Security Council resolution 1373 (2001): Threats to International Peace and Security caused by Terrorist Acts.

4. Details can also be found in the code of practice on security in ports: Tripartite Meeting of Experts on Security, Safety and Health in Ports – Geneva 2003