IMO

INTERNATIONAL MARITIME LAW INSTITUTE

Established under the auspices of the International Maritime Organization

A specialized agency of the United Nations

IMLI

A SUBSIDIARY LEGISLATION TO IMPLEMENT THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE INTO THE LAWS OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

A Legislation Drafting Project submitted in partial fulfillment of the requirements for the award of the Degree of Master of Laws (LL.M.) in International Maritime Law at the IMO International Maritime Law Institute

Submitted By: LCDR SANCHALA PERERA

(SRI LANKA)

Supervisor: DR. SANJEET RUHAL

Academic Year: 2020/2021

Table of Contents

LIST OF ABBREVIATIONS

CSO - Company Security Officer

DOS - Declaration of Security

ILO - International Labour Organization

IMO - International Maritime Organization

ISSC - International Ship Security Certificate

ISPS - International Ship and Port Facility Security

LTTE - Liberation Tigers of Tamil Eelam

MSC - Maritime Safety Committee

PFSA - Port Facility Security Assessment

PFSP - Port Facility Security Plan

PFSO - Port Facility Security Officer

RSO - Recognized Security Organization

SOLAS - Safety of Life at Sea

SSA - Ship Security Assessment

SSAS - Ship Security Alert System

SSP - Ship Security Plan

SSO - Ship Security Officer

SUA - Suppression of Unlawful Acts against the Safety of Maritime Navigation

WCO - World Customs Organization

UN - United Nation

Explanatory Note on Proposed Regulation to Implement the International Ship and Port Facility Security (ISPS) Code, 2004

Introduction

The 9/11 attack on the World Trade Centre is one of the most unfortunate events in world history in the 21st century. With this event, the international community realized, especially the West, the impact of global terrorism, which is not limited to single state or region. Terrorist anywhere in the world is a danger to the entire international community. It is also important to note that not only a ship or aircraft need to be protected, but they could be used as a weapon of mass destruction. Securing the ocean was the most challenging task to the whole world as there was no such instrument was in place to secure the ports and ships from such unprecedented threats.

Therefore, the International Ship and Port Facility Security (ISPS) Code was adopted at a Diplomatic Conference on Maritime Security which was held at the headquarters of the International Maritime Organization (IMO) in December 2002[1] as a response to implement preventive security measures to protect both merchant ships and seaports. Due to the high necessity and the urgent consideration of implementing security measures motivated multilateral reform within the IMO; only after 18 months of its adoption the ISPS Code came in to force with effect from 1 July 2004 with the immense contribution of Maritime Safety Committee (MSC) and its Maritime Security Working Group.

Aforementioned Conference adopted a number of amendments to the International Convention for the Safety of Life at Sea (SOLAS) 1974 and the adoption of the ISPS Code is one of the key developments in addressing ship and port security. With the introduction of ISPS Code, SOLAS Convention was extended its scope beyond Maritime Safety to Maritime Security under Chapter XI. Hence SOLAS Convention Chapter XI split into 2 new chapters namely Chapter XI-1 and Chapter XI-2. Accordingly, Chapter XI-1 deals with special measures to enhance maritime safety while Chapter XI-2 provides special measures to enhance maritime security. This new Chapter XI-2 is the ISPS Code.[2] The Conference further adopted 'a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the ISPS Code and pave the way for future work on the subject.'[3]

IMO has initiated steps to assist Contracting Governments in exercising their implementation of the various aspects of the ISPS Code such as model training courses, issuance of specific guidance via MSC Circulars, organizing regional and national workshops and the conduct

[1] IMO (Maritime Security Manual of the Maritime Safety Committee) 'Measures to Enhance Maritime Security' (5 March 2001) MSC 89/INF.13.

[2] Kamrul Hossain, Hugh M. Kindred, and Mary R. Brooks, 'The Challenge of Maritime Security against Terrorism: A Dialogue Between the European Union and Canada' in Timo Koivurova and others (eds), Understanding and strengthening European Union-Canada relations in law of the sea and ocean governance (Lapin yliopisto and Arktinen keskus 2009) 354.

[3] IMO (n 1).

of advisory and assessment missions at the requests of each government.[4] Only States who are Contracting Governments to SOLAS have a legal obligation to comply with the requirements of the ISPS Code and to submit information to IMO.

Ship and port facility security are considered the solemn components of present-day maritime security,[5] hence the ISPS Code provides a broad set of measurements to enhance international security by assigning responsibilities to all stake holders including Contracting Governments, Port Authorities, Shipping Companies. Further 'it is the most comprehensive effort to institutionalize a global culture of maritime security'[6] and it is applicable to all shipping nations around the globe.

The ISPS Code is divided into two divisions as part 'A' and 'B'. Part 'A' is mandatory and it contains thirteen requirements in relation to port security which SOLAS Contracting Governments should comply with and part 'B' of the Code detailed recommendatory guidelines on how to cope with the specifications stated in part 'A' of the Code. The recommendatory part 'B' is 'intended to address those areas where very specific characteristics of a ship or port facility may mean that "one size" does not "fit all".'[7]

Security is not a stable factor, and therefore security threats are subjected to change, and it is the responsibility of the Contracting Governments to promulgate relevant guidelines in relation to ships and port facilities, communicate information among the stake-holders, constant observation and take instant response whenever the requirement arises. Therefore the ISPS Code can be taken as an example which stands for states collaboration to enhance maritime security, reflecting the shared interest among states and to curb greater number of security threats arise against both ports and ships.[8]

1. Historical Background of the ISPS Code

As mentioned above, before the emergence of the Code maritime industry in the world came under increasing maritime threats which hugely affected to both ships and ports. Most of the maritime catastrophes were able to give birth to certain international conventions. The tragedy of *Titanic* which perished the number of lives of passengers and crew due to inadequate safety equipment prevailed in the ship at the time of the accident. This incident becomes one of the turning

[4] ibid.
[5] James Kraska, 'Ship and Port Facility Security' in David J Attard and others (eds), THE IMLI MANUAL ON INTERNATIONAL MARITIME LAW VOL III Shipping Law (OUP 2016) 442.
[6] ibid, 444.
[7] IMO, 'Frequently Asked Questions on Maritime Security' (IMO work and Maritime Security) < https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx> accessed 7 January 2021.
[8] Natalie Klein, Terrorism and Proliferation of Weapons of Mass Destruction: Maritime Security and the Law of the Sea (OSAIL 2012) 149.

points in the maritime industry, which paved the way to emerge international legal frame work on the safety of the ships, passengers and the crew onboard.

In the ancient days, merchant ships were given opportunities enter to the ports without much hindrance, but due to the easy access to ports, terrorists have been used merchant ships as a tool as well as a means of transporting the terrorists along with their weapons or sometimes ship itself as a weapon. Hijacking of gas ships and blowing up in busy seaports can be given as an example.[9] Further, the hijacking of the Portuguese passenger ship, namely *Santa Maria* is considered the first case of maritime terrorism which was occurred on 22 January, 1961; 24 leftist Portuguese terrorists hijacked the luxury cruise liner, which carried 600 passengers and a crew of 300.[10]

In 1985 Palestine Liberation Front terrorists hijacked an Italian cruise ship and killed an elderly American passenger off the coast of Egypt, and this is known as *Achille Lauro* incident. Since then terrorist activities against vessels have become more common. Following the *Achille Lauro*, in December 1985, the United Nations General Assembly requested the IMO to do an advance study on this matter and make recommendations on appropriate measures.[11] Subsequently in 1986 the IMO issued guidelines on 'Measures to prevent unlawful acts against passengers and crews on board ships' via MSC/Circ.443.[12] As a result of the incredible efforts of the IMO Legal Committee in March 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) was adopted.[13]

Another terrorist incident was reported in 1988 where gunmen boarded a cruise ferry; opened fire, and that killed 9 people in the ferry in the *City of Poros*.[14] In 2000 *USS Cole*, a US Navy destroyer berthed at Eden in Yemen came under a suicide attack. An explosive laden small boat rammed into the ship, causing heavy casualty and damages to the ship. A similar incident was again reported in Yemen in 2002 against *MT Limburg* crude carrier was attacked while entering the Yemen port of Dhaba.[15] As per the records, there were 212 reported maritime terrorism incidents took place from 11 June, 1970 to the date which the ISPS Code came into operation.[16]

---

[9] Lars H. Bergqvist, 'THE ISPS-CODE AND MARITIME TERRORISM' (Centre for International Maritime Security, 15 July 2014) <http://cimsec.org/isps-code-maritime-terrorism> accessed 24 November 2020.

[10] ibid.

[11] IMO (n 7).

[12] ibid.

[13] ibid.

[14] Iliana Christodoulou-Varotsi and Dmitry A. Pentsov, *Maritime Work Law Fundamentals: Responsible Shipowners, Reliable Seafarers*: *The International Ship and Port Facility (ISPS) Code* (978-3-540-72751-4, Springer 2008) 665.

[15] Jayanath Colombage, 'Maritime security and port facility security code' (Sri Lanka Business News, 5 July 2011) <http://archives.dailynews.lk/2011/07/05/bus19.asp> accessed 24 November 2020.

[16] Bergqvist (n 9).

Despite all these incidents that happened previously, 9/11 attacks in New York became the corner-stone of the creation of ISPS Code. In the catastrophe of 9/11 attacks hijacked aircrafts flew into the twin towers of the World Trade Center, destroyed part of the Pentagon and crashed on a field in Pennsylvania. For these disastrous attacks, the terrorists used aircrafts to reach US targets and similarly ship itself can be commonly utilized as a weapon for future calamities. Quick response of international community as well as the weight of the U.S.'s influence; the IMO took initiatives in November 2001 at the IMO's 22nd Assembly; adopted a resolution A.924 (22)[17] to review the procedures to avert the acts of terrorism and safeguard the passengers and crews as well as the safety of ships. Further, the IMO promulgated the ISPS Code is very much similar to the US Maritime Transportation Security Act, which came into operation in 2002.[18]

2. Structure and the Importance of the ISPS Code

(a) The Objectives of the ISPS Code

The ISPS Code basically engages with the security aspects of the ships, ports and port employees and to undertake preventive security measures if any threat has been identified. Apart from the primary objective discussed in the introduction, the rest of the objectives of the Code can be listed as follows:

- to establish the respective roles and responsibilities of all parties concerned with safeguarding maritime security in ports and on board ships, at the national, regional and international levels;
- to ensure that there is early and efficient collection and exchange of maritime security-related information, at national, regional and international levels;
- to provide a methodology for ship and port security assessments, which facilitates the development of ship, company and port facility security plans and procedures, which must be utilized to respond to ships' or ports' varying security levels; and
- to ensure that adequate and proportionate maritime security measures are in place on board ships and in ports.[19]

In order to reach the above objectives, the Contracting Governments, Port Authorities and Shipping Companies are required to appoint capable Security Officers. For each ship, Ship Security Officer (SSO) to be appointed; for shipping Company, Company Security Officer (CSO) to be

[17] IMO (n 7).

[18] Jibkwon Jeong, 'Progress and challenges: ten years after the ISPS code' (2013) The Maritime Commons: Digital Repository of the World Maritime University 8-9 <https://commons.wmu.se/cgi/viewcontent.cgi?article=1341&context=all_dissertations> accessed 6 February 2021.

[19] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Part A 1.2.

appointed and Port Facility Security Officer (PFSO) to be appointed for the port facilities. They are responsible for preparing and implementing effective security plans and further to manage any potential security threats.[20]

(b) The Application and the Requirements of the ISPS Code

In order to fulfill the aforementioned objectives, the ISPS Code stated some functional requirements such as:

- to collect information in relation to security aspects from the relevant authorities of the contracting government
- to evaluate the collected information
- to share the information in relation to security among relevant authorities of the contracting government
- establish proper communication mechanisms among ships and port facilities to rapid exchange of information
- to implement accurate security plans between ports and ships based on security assessments[21]

The ISPS Code is applicable for all passenger ships include high speed passenger crafts, cargo ships of 500 gross tonnage and more, mobile off-shore drilling units and Port facilities serving ships sailing on international voyages.[22] Although over 98 per cent of the world's shipping operates under the SOLAS Convention; the ISPS Code does not apply to warships, any government ships which are utilized for non-commercial purposes, ships less than 500 gross tonnage and for any fishing vessel.[23] In the case of *USS Cole* the suicide craft was either not fallen under the ISPS Code or identified as a security threat. Therefore, the IMO has initiated to address such threats over the adoption of non-mandatory guidelines on security aspects of vessels which do not cover either in the ISPS Code or the other amendments to the SOLAS Convention.[24]

(c) Structure and Implementation of the ISPS Code

As a result of different types and sizes of ships and ports; the ISPS Code does not specifically mention the precise guidelines that each ship and port should adhere, but it has

[20] International maritime organization, 'SOLAS XI-2 and the ISPS Code' (IMO work and Maritime Security) <https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI2%20ISPS%20Code.aspx#:~:text=The%20International%20Ship%20and%20Port, security%20regime%20for%20internatio> accessed 24 November 2020.
[21] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Part A 1.3.
[22] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Part A 3.1.
[23] Klein (n 8) 153.
[24] ibid.

produced a uniform frame that assessing and reacting to security threats. As it is mentioned at the beginning of this chapter part 'A' of the ISPS Code mandates that each port to;

- appoint a PFSO
- conduct a comprehensive Port Facility Security Assessment (PFSA)
- prepare Port Facility Security Plan (PFSP)
- appoint a Company Security Officer (CSO)
- inspect each ship and appoint a Ship Security Officer (SSO)
- prepare a Ship Security Assessment(SSA)
- prepare Ship Security Plan (SSP)

Part 'B' of the ISPS Code deals with the primary obligations to protect the ships when they are berthed and enjoying port facilities.[25]

The ISPS Code has assigned a multiplicity of roles to Port States, Coastal States, and Flag States, and also to certain entities assigned as PFSOs, CSOs, and SSOs. The Particular duties of each entity are set forth in the ISPS Code and also it is proposed to enhance communication and cooperation among the aforementioned entities.

The SOLAS Convention previously did not apply to a port facility, but it is essential to review the provisions in relation to the port facility under the ISPS Code; deemed necessary to ensure that the ports are protected from the threats ascend out of the sea as well as ashore. The PFSO should also pay close attention to all types of security threats that may arise from the ships arriving to respective ports after international voyage. Further, it is the duty of the PFSO to set out appropriate security levels for the ships in respective territorial waters.

When take into account the provisions in the ISPS Code in relation to the role of SSO over the ships; the Company must train a competent officer as SSO and that particular SSO is responsible for the security of the ship, conduct frequent drills as per SSP and accountable over the acts of the crew with regard to ship security. The timely and frequent assessment of the SSP by SSO is essential for finding shortcomings and enhancing the current SSP in response to changes in ship operations, structure, or as a consequence of failing a drill exercises.[26] The SSA also be documented, reviewed, accepted and retained by the Company.

The CSO is appointed by the Company and is responsible for the SSA and for the onboard survey to confirm the development and implementation of the SSP. If there is any discrepancy observed, it is the duty of the CSO to liaise with the non-conformities and to alter the SSP. The SSP is a plan which is placed onboard the ship which indicates the duties of the crew at three security levels. Further it is included the things that should be done and should not be done at the different

[25] Colombage (n 15).
[26] Kraska (n 5) 450.

types of threats. Every ship must carry a SSP, approved by their respective Administration who is responsible for reviewing and approving a SSP for the ship. Finally, the SSO is responsible for CSO to enforce the SSP onboard the ship.[27]

The PFSO is appointed by the Contracting Government and is responsible for preparing, implementing and monitoring the efficacy and applicability of the approved PFSP which comprises independent internal audits in respect of the application of the plan[28] and further effectiveness can be evaluate by the relevant Authorities. The PFSO is responsible for conducting PFSA and it is an essential part which combines with the PFSP. The PFSA is usually assessed and review by the respective Authority which the Contracting Government has been nominated. The PFSP contains the minimum operational and physical security measures the port facility shall take at all times. The amendments can be brought to the approved plans and for the main amendments, it is necessary to obtain the respective Authority's re-approval.[29] The IMO has established the ISPS Code database section, and accordingly, that section has listed the ports which comprehend the approved PFSPs.[30]

Achieving the comprehensive implementation of the ISPS Code is quite challenging; some states struggle to comply with the Code's provisions. But it has already accomplished a global effect by linking ship and port facility security between governments and commercial entities in an attractive manner. This Code closely relates to World Customs Organization (WCO) and the International Labour Organization (ILO). Hence 'these three interlocking international organizations IMO, WCO, and ILO create an institutional rule set for protecting the global cargo supply.'[31]

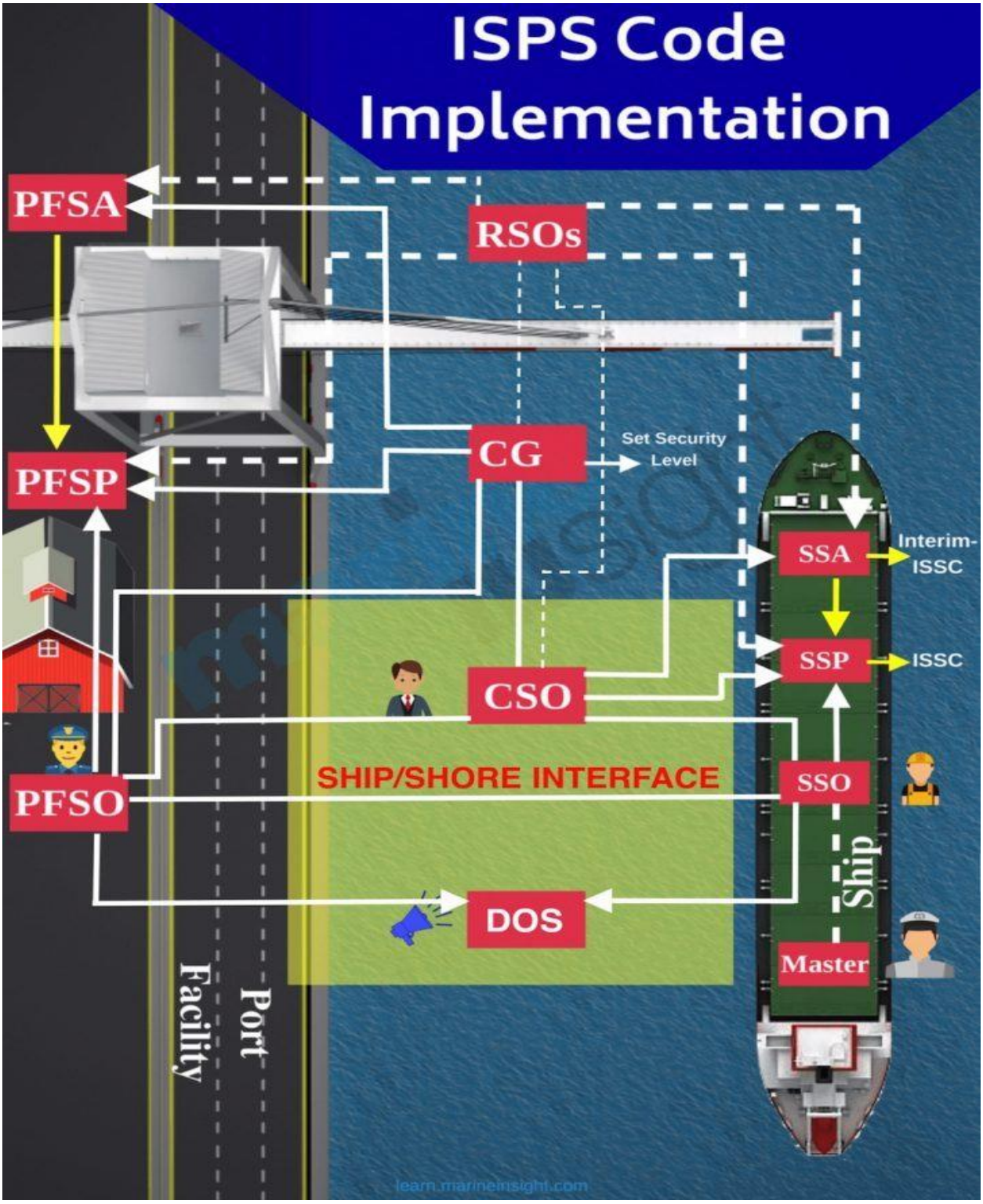
After the inception of the ISPS Code, SOLAS Contracting Governments, Companies, Port facilities, and Ships are responsible for implementing the Code. Given this comprehensive range of special measures to enhance security promulgated by the IMO with the initiatives of MSC and its subsidiary bodies to achieve the efficiency of shipping. Some of the critical IMO measures listed as follows;

- MSC/Circ.1110 on 'Matters related to SOLAS regulations XI-2/6 and XI-2/7'
- MSC/Circ.1111 on 'Guidance relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code'
- MSC/Circ.1112 on 'Shore Leave and Access to Ships under the ISPS Code'

[27] Anish, 'The ISPS Code For Ships – An Essential Quick Guide' (Marine insight, 11 September 2019) <https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/> accessed 22 November 2020.
[28] Jan E de Boer, 'The IMO: Maritime Terrorism/ Security and Global Ocean Governance' in David J Attard and Donald W Greig (eds), *THE IMLI TREATISE ON GLOBAL OCEAN GOVERNANCE* Vol III IMO and Global Ocean Governance (OUP 2018) 166.
[29] ibid.
[30] IMO (n 7).
[31] Kraska (n 5) 449.

- MSC/Circ.1156 on 'Guidance on the access of public authorities, emergency response services and pilots on board ships to which SOLAS Chapter XI-2 and the ISPS Code apply'[32]

[32] de Boer (n 28) 167.



Anish, [Image of ISPS Code Implementation] 'The ISPS Code For Ships – An Essential Quick Guide' (Marine insight, 11 September 2019) <https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/> accessed 22 November 2020.

(d) Ships and Ports Security

There are many threats to the ships and ports in various scales. When recollecting the past terrorist attacks at sea it is observed that terrorists plan well ahead of an operation, in which they monitor the ships and port facilities before launching an attack. They might recruit crew members or port employees and plant their agent in ports and ships, making all ships and port facilities are vulnerable to terrorist attacks especially the cargo ships are more exposed than passenger ships.[33] Therefore, controlling the access to ship or port facility is far more essential. Terrorism is not the only threat to maritime security. Cargo theft, stowaways, drugs and weapon smuggling and piracy too can be identified as non- terrorism related threats.[34]

As per Regulation XI-2/3 of the Code it requires Administrations to set security levels and ensure the provision of security level information to ships entitled to fly their flag. Further, every port facility and ship should prepare a PFSP and SSP depicting three levels of security as mandated in the code; under the code designated levels of security as follows;

- Security Level 1 (Normal): Minimum appropriate protective security measures to be maintained at all times
- Security Level 2 (Increased): Appropriate additional protective security measures which shall be maintained for a period owing to a heightened risk of a security incident
- Security Level 3 (High): Further specific protective security measures maintained for a limited period when a security incident is probable or imminent [35]

Within the territory of a Contracting Government and prior to entering a port, a ship shall comply with the security level set by that Contracting Government and it is the responsibility of the SSO to implement that particular security level. The security level adopted for the port facility by the Contacting Government must be informed to ship Administration as a sign of cooperation. In some instances, the Designated Authority in relation to ports and the Administration in relation to ships are set a security level based on the degree of risk prevailed at the time of the security incident.[36] Hence the security level generates 'a link between the ship and the port facility, since it triggers the implementation of appropriate security measures for the ship and for the port facility.'[37]

Since the date the Code came into operation, it is mandatory for all Shipping Companies to obtain an International Ship Security Certificate (ISSC) from an accredited Shipping Society.[38] If unable to produce such an ISSC without any reasonable grounds, then that ship is not in compliance

[33] Colombage (n 15).
[34] ibid.
[35] ibid.
[36] Kraska (n 5) 453.
[37] IMO (n 7).
[38] Hossain (n 2) 355.

with the requirements of part 'A' of the ISPS Code. Therefore certain control measures could be taken by the Port State, such as:

- inspection of the ship
- delay the ship
- detention of the ship
- restrict on the ship operations
- expulsion from port
- movement of the ship within the port
- denial of port entry
- impose less severe administrative remedies[39]

Another important factor to be discussed under part 'B' of the Code is a Declaration of Security (DOS). DOS is 'an agreement between a ship and another ship, or between a ship and a port facility, with which it interfaces, specifying the security measures each will implement during the period of time they will interact'[40] and ships should have their DOS available for inspection for the period covering the previous ten ports of call.

When discussing the security equipment mentioned in the Code, there are different types of security equipment such as metal detector for checking the person entering the vessel, Ship Security Alert System (SSAS) are kept on board. Minimum Security equipment like scanner and metal detector are available at all times with the port facility in order to maintain firm security inside the port. According to Regulation XI-2/6 of the Code, it is mandated that every ship must have installed a SSAS, which do not sound on the ship but alarms the shore authority about the security threat.[41]

(e) Contracting Government and the Designated Authority and Recognized Security Organizations

The Contracting Government has the right to decide the extent and application of part 'A' of the Code. Further, the Contracting Governments have overall responsibility over the Maritime Security and therefore Contracting Governments can establish Designated Authorities within governments to accomplish their security responsibilities and also may delegate certain responsibilities to non-governmental Recognized Security Organizations (RSO).[42]

The Contracting Governments are required to undertake PFSAs in their respective ports. Due to the power vested with the Contracting governments, these assessments shall be undertaken either to a designated authority or the RSO. The PFSAs will need to be reviewed periodically. The

[39] Kraska (n 5) 457.
[40] ibid, 458.
[41] Anish (n 27).
[42] Hossain (n 2) 355.

results of the PFSA have to be approved by the Contracting Government or the Designated Authority, and based on the PFSA; it is determining which port facilities are required to appoint a PFSO. The PFSP has to be approved by the port facility's Contracting Government or by the Designated Authority. Further, the PFSP sets forth the conditions under which a port facility will request ships to comply with a DOS.[43]

The Contracting Governments are responsible for deciding the time of the DOS is required for ships flying their flags and ports under their authority, subject to the risk of the collaboration between ships and ports. The Designated Authority privilege in determining the circumstances requiring a DOS, but RSO does not privilege for the same authority in this regard.[44]

To reach the objectives of the Code along with ship and port facility operations the Contracting Government has to work together, unless it would not be able to reach the expected security level. Therefore this Code is expected from the Contracting Governments to collect and evaluate the information on security threats and share the relevant facts with other Contracting Governments.

Though the Security levels are set by the Contracting Government and generally it can be delegated to the Designated Authority. Therefore the Designated Authority usually acts as a mode of implementing the Code. The Designated Authority has entire responsibility over port facilities and at first, must undertake PFSA. The PFSA involves with the port premises, inspection of the relevant documents, records, plans and scrutinize port security equipment. Appointing a suitable PFSO and preparation of a PFSP are followed by the PFSA.

The Contracting Government or the Designated Authority may delegate part of their duties to RSOs. To approve the ship security plans, verification for ships, issuance and endorsement of ISSCs are some of the duties performed by the RSOs. Sometimes the SSP may be prepared by an RSO on behalf of CSO.[45] The responsibilities of RSOs are technical in nature; hence the knowledge on ship and port operations is essential and also it is more beneficial if the RSO have undergone the experience of security threats. Therefore former military officers are more capable of enlisting as RSOs.[46]

(f) Port State Responsibilities on Implementation of the ISPS Code

As per the ISPS Code, a Port State requires that ships prior to enter into the waters of respective Port State need to compliance with Chapter XI-2 of SOLAS Convention and ISPS Code such as ship should possess the ISSC with the aim of preventing impose control measures against

[43] Kraska (n 5) 456.
[44] ibid, 458.
[45] ibid, 461.
[46] ibid, 462.

non-compliance. The Ports States, via their respective Contracting Governments determine the Security levels for their ports. Further a Port State requires a DOS from a ship to provide port facility. A Port State has entire discretion in admitting foreign vessels into its ports as well as to internal waters, while all nations have a responsibility to render the assistance to refuge for ships. Further 'The port State's criminal law or civil code may apply to foreign-flagged ships calling on ports of the state. Foreign-flagged ships are under obligation to provide information on the vessel, cargoes, and passengers, to the port State's Designated Authority or Administration.'[47]

Prevailing pandemics like Coronavirus (Covid-19) would exist in the world for another couple of years and in future also more menace would come up and those would badly affect for the effective function of the Port State to provide an incredible service. Though this is not a security threat, it would be indirectly become a security threat. As a response, the IMO has promulgated a Circular for Port State Control (PSC) regimes on harmonized actions at the time of pandemic of Covid-19[48] had given some important guidance for the Port States to comply with to overcome this pandemic.

(g) Flag State Responsibilities on Implementation of the ISPS Code

As per Chapter XI-2 of SOLAS Convention and part 'A' of the ISPS Code, Flag States should ensure that ships flying under their respective flags comply with internationally established standards. The responsibilities of the Flag State are generally assumed by the respective Maritime Administration of each State. Accordingly, the Administration is responsible for assuring that their ships are in compliance with the aforementioned international standards and performing the following responsibilities; approves the SSPs, issues the ISSCs to their ships, develops a DOS to clarify the duties between the port facility and the ship and assessing security threats and setting security levels as appropriate for their ships.[49]

(h) Responsibilities of Shipping Companies on Implementation of the ISPS Code

According to the ISPS Code, Shipping Companies should appoint CSO for each fleet and SSOs for each ship. They should carryout SSA for each ship; the documents should be retained in the ship and prepare the SSP for each ship. The SSPs are subject to the approval of the Administration of the Flag State. The Companies also should work in harmony and render their support to CSO, SSO and the crew of the ship to fulfill their duties and responsibilities. Shipping

[47] ibid, 457.
[48] IMO 'Coronavirus (COVID 19) – Third video meeting for Port State Control (PSC) regimes on harmonized actions at the time of pandemic of Covid-19' (22 December 2020) Circular Letter No.4204/Add.37.
[49] Klein (n 8) 154.

Companies are further 'responsible for ensuring that each ship security plan 'contains a clear statement emphasizing the master's authority' over the vessel.'[50]

3. Changes brought with the ISPS Code

After 1 July 2004, since the Code came into operation, new international framework has been established to co-operate among the Contracting Governments, ships and port facilities to detect security threats in the maritime transport sector. One of the most significant changes is that the Contracting Governments are competent to exercise their control over the ships in compliance with Chapter XI-2 of the SOLAS Convention and the ISPS Code.[51] Further, the ISPS Code covers that the Contracting Governments are obliged to confirm that the conducted PFSAs and PFSPs are developed, implemented, and reviewed in accordance with the Code.[52]

4. Advantages and Disadvantages of the ISPS Code

With the inception of the ISPS Code new international standard framework has been established to assess risks addressing to security issues between the ships and ports which is one of the key benefits of the Code. As per the review published by the Paris and Tokyo Memorandum of Understandings in relation to Port State Control, has shown positive remarks over the implementation of the Code.[53]

There are some other prospective commercial benefits to the entire shipping industry; by initiating an effective security regime ports would be able to participate fully in global trade,[54] better documentation procedure, secured working environment established for seafarers and port workers, reduction of the incidents in respect of thefts and accidents. A significant example of such advantages is that there was a considerable decrease in reported stowaway cases in US ports during the first six months after the inception of the ISPS Code.[55]

Even though, the Code has established a wide-range of practices for the security of ships and port facilities; there is a lack of consideration given to the seafarers who play a major role in international trade where they have been given with extra workload related to the implementation of the ISPS.[56] Slow work progress when the security level rises, inadequate paperwork and certification requirements, lack of operating costs of ships and ports at the high security level[57] are some other disadvantages of the ISPS Code. While the Code focused on preventing and minimizing

[50] Kraska (n 5) 460.
[51] Colombage (n 15).
[52] de Boer (n 28) 162.
[53] ibid, 171.
[54] IMO (n 7).
[55] IMO (n 1).
[56] Hossain (n 2) 353.
[57] Anish (n 27).

the terrorist attacks; it is silent in responding to security incidents.[58] Another disadvantage is the Code mainly addressed to the physical security of the port facility and vessel but not focused on the container security. Therefore security incidents like the smuggling of drugs would not be declined as a result of the drugs are concealed within the containers. [59]

5. Challenges of Implementing the ISPS Code

Legislations those come into operation has its own challenges, and the ISPS Code is no different, and the following challenges can be considered.

- due to the security threats, many countries are prohibiting shore leave for seafarers and that affects the human rights of the seafarers
- effect on the daily activities of the crew due to perform additional duties in relation to security
- the port activities are affected when the security level rises and that leads to slow down of cargo operation
- some ports do not permit any cargo operations under security level 3 until reduce the security level[60]
- to implement the provisions to strengthen and protect the efficiency of the ships and port facilities during the times of pandemics such as Covid -19
- lack of national legislation/guidelines on ISPS Code implementation
- the ISPS Code as a mean to address all maritime security threats such as piracy and stowaways that are much more of real threats than terrorism[61]
- part 'A' of the Code is only mandatory and it comprises one third of the Code; in order to provide effective port security, there is a shortage of the application of dynamic port security measures[62]
- lack of standardization at port facilities due to recommendatory part 'B' is significantly varied in different countries[63]

The Code was developed to protect the international community against terrorism. Although there are positive impacts of the Code some serious incidents have been reported after implementing the Code such as the attack to *Don Ramon* in 2005, the explosion of *M Star* in 2010.[64]

---

[58] Jeong (n 18) 56.
[59] ibid 49.
[60] Anish (n 27).
[61] Bergqvist (n 9).
[62] Stephen Cox, 'THE ADVENT AND FUTURE OF INTERNATIONAL PORT SECURITY LAW' (2013) 1(1) NSLJ <https://www.nslj.org/pdfs/NSLJ_Vol1_Iss1_Spring2013_Cox_77-123.pdf > accessed 6 February 2021.
[63] Jeong (n 18) 57.
[64] Bergqvist (n 9).

6. Sri Lanka's Obligations towards Establishing a Legal Framework to Implement the ISPS Code

Start with the fact that Sri Lanka is an island in the South Asian Region; a strategically located hub of the Indian Ocean and maritime has been the most important source of international transportation and communication. Sri Lanka has a long history in maritime related activities. Though, Sri Lanka had experienced three decades of civil conflict with the terrorist group of Liberation Tigers of Tamil Elam (LTTE); Sri Lankan ports were never closed and sea lanes were kept open throughout the time.[65] Further, Sri Lanka being the maritime hub in South Asia for transit cargo ensured safe passage for merchant ships operates in Sri Lankan waters.

Furthermore, Sri Lanka being situated middle of the sea lane of communication connecting East and West, Sri Lanka is potential for non-terrorism threats like drug trafficking and human smuggling. That may indirectly affect national security, and therefore firm security measures are required to combat such illegal activities. The significant positioning of Sri Lanka comes with a great obligation to prevent the aforementioned crimes, ensure the safe passage of merchant ships and prevent terrorist activities. According to the ISPS Code Regulation XI- 2/7 it is guided that threats to ships at sea and the measures to be adopted by a littoral state.[66] Fortunately, because of strict security measures implemented by the Sri Lanka navy to counter terrorism, the rate of maritime crimes that occurred in Sri Lankan waters was at a lower level.[67]

As is discussed above, the ISPS Code is an amendment to Chapter XI of the SOLAS Convention and which was in operation since 1 July 2004 all over the world, including Sri Lanka. After adopting the Maritime Security Measures in December 2002, the IMO has facilitated and taken administrative and organizational alterations to implement the Maritime Security Measures in National Legislations.[68]

Although Sri Lanka does not possess a legislative instrument implementing the ISPS Code, Commander of Navy was appointed as the Designated Authority for implementing part 'A' of the ISPS Code by the Minister of Ports and Aviation via Ministry of Ports and Aviation letter No.AD/2 M14 dated 20 May 2004 as per the directive of IMO. Area Commanders of respective naval areas were appointed as Competent Authority for major ports as depicted in Sri Lankan map. They were directed to prepare PFSA as per the directives promulgated in the ISPS Code and submitted to Designated Authority. Subsequently, PFSOs were appointed and PFSOs had to submit PFSPs to the Designated Authority. Finally, the ISPS Code fully came into operation in Sri Lanka with effect from 14 June 2004 on a trial basis.[69] Since 30 June 2004, Sri Lanka has not entertained Merchant

[65] Colombage (n 15).
[66] IMO (n 7).
[67] Colombage (n 15).
[68] IMO (n 1).
[69] Colombage (n 15).

Ships that do not possess an ISSC issued by their respective Flag States. Further, the port facility operators are instructed to check the compliance of the Code before they undertake to provide services to vessels.[70]

In June 2016, the MSC, in its 96th session approved guidance for developing and implementing National Maritime Security Legislation. This was further expected to assist SOLAS Contracting Governments to fully implement the Chapter XI-2 of the SOLAS Convention.[71] Even prior to the said guidance, many Asian countries, including India, Malaysia, Singapore and Hong Kong have drafted national laws based on the ISPS Code except Sri Lanka.

India has promulgated circular prescribing guidelines for implementing the ISPS Code on 27 October 2004[72] within a short period of time after the world-wide implementation of the ISPS Code. Malaysian implemented the ISPS Code in 2004; the Malaysian Marine Department is appointed as the Designated Authority.[73] On 29 June 2004, the ISPS Code implemented in Hong Kong via CAP 582A Merchant Shipping (Security of Ships and Port Facilities) Rules.[74] Further, the Marine Department of the Hong Kong Special Administrative Region appointed as the Designated Authority to undertake the security of ports.[75]

When comparing the Sri Lankan context with the above countries, the Designated Authorities in those countries are different from the Sri Lankan Designated Authority. The rationale behind appointing the Commander of Sri Lanka Navy as Designated Authority, due to the strategic location where Sri Lanka is situated and the Sri Lanka Navy being the 1st line of defence in Sri Lanka.

During the period of war, the land road network was almost damaged or blocked by Government forces on security concern and all supplies to the Military and civilians in Northern Sri Lanka were transported by sea. All the logistics items such as medicine, essential food items, fuel transported by the Navy or under the protection of the Navy. LTTE had made several attempts to attack ships carrying cargo for civilians in Northern Sri Lanka, such as *Princess Wave* in August

---

[70] Sri Lanka Shippers' Council, 'Implementation of the International Port Facility Security Code' (Merchant Shipping Division, 11 June 2004) <http://www.shipperscouncil.lk/archives/articles/2004/merchant-shipping-notice.htm> accessed 10 January 2021.

[71] de Boer (n 28) 171.

[72] Director General Shipping, 'ISPS Code Application for Coastal Vessels' (27 October 2004) <https://dgshipping.gov.in/WriteReadData/userfiles/file/ISPS%20Circular123456.pdf> accessed 6 March 2021.

[73] Asian Organization, 'Implementation of the ISPS Code' (Asian Regional Forum, Annex 21) <https://aseanregionalforum.asean.org/wp-content/uploads/2019/03/Annex-21-Implementation-of-ISPS-Code-presentation-by-Malaysia-5th-ism-on-ms.pdf> accessed 7 March 2021.

[74] <https://www.elegislation.gov.hk/hk/cap582A!en> accessed 7 March 2021.

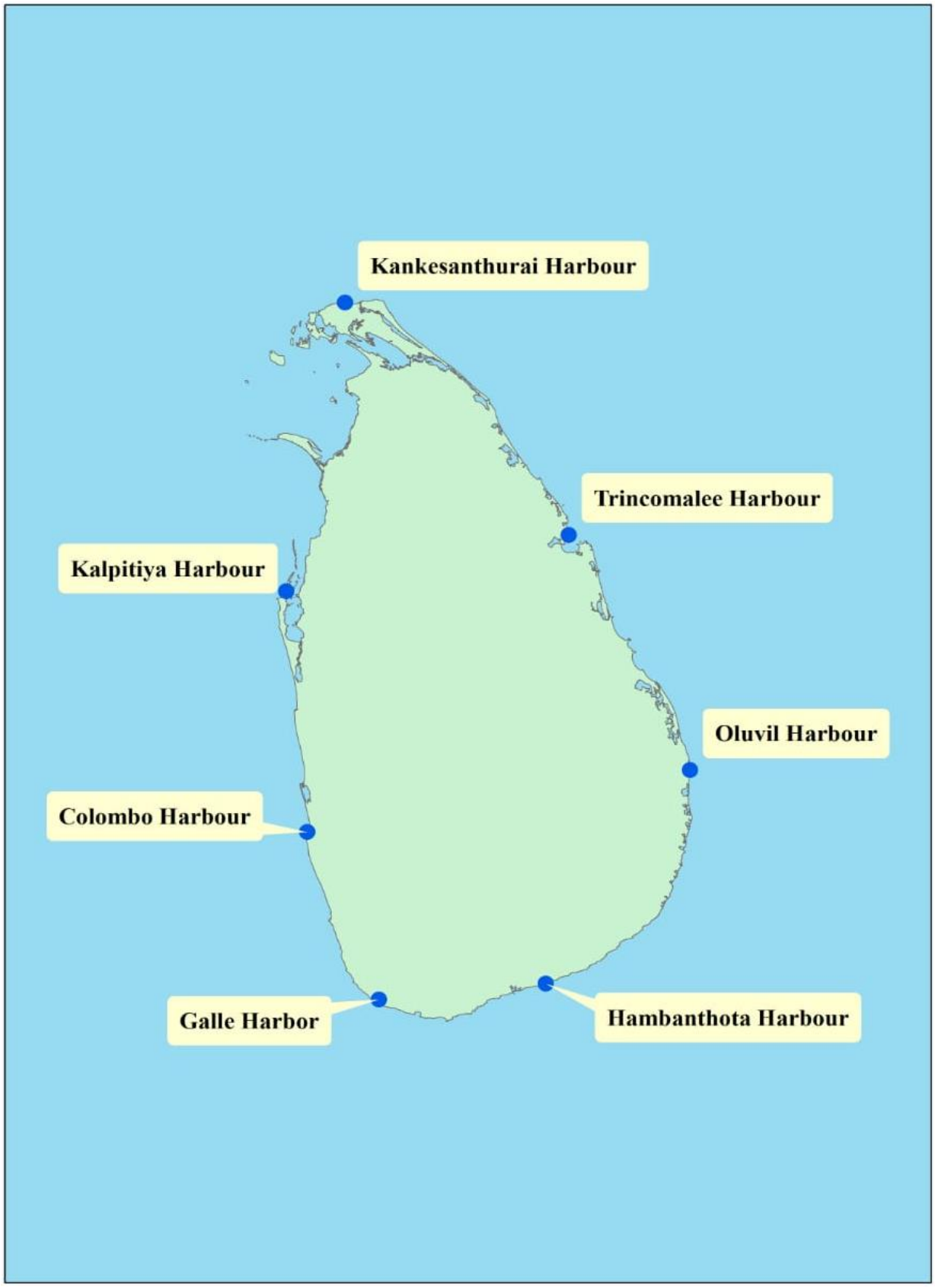
[75] Marine Department, 'General' (The Government of the Hong Kong Special Administrative Region) <https://marsec.mardep.gov.hk/en/general.html#:~:text=Marine%20Department%20of%20the%20Hong,the%20port%20as%20a%20whole> accessed 7 March 2021.

1996 and *Princess Kash* in August 1998[76] are few examples for it. The LTTE had carried out suicide attacks against the naval ships berthed at Trincomalee, Kankasanthurei and Kareinagar and tried to destroy the merchant ships berthed at Kankasanthurei and Colombo harbours. However, effective security measures implemented by the Sri Lanka Navy managed to prevent LTTE attacks which aimed to destabilize the country's economy through disturbing efficient functioning of commercial harbours in the country. These factors have proved that although Sri Lankan ports have been under terrorist threat for almost three decades, Sri Lankan ports were able to survive, managed and functioned well.

According to the information gathered from Sri Lanka Navy, presently, seven harbours in Sri Lanka, namely Colombo, Galle, Hambanthota, Oluvil, Trincomalee, Kankasanthurei and Kalpittya, are functioning as per the directives promulgated in the Chapter XI-2 of SOLAS Convention; the ISPS Code, Sri Lanka Navy performing the port facility security duties. Further, ISPS Officers are being appointed to assist the PFSOs for the smooth function of the port facility. Former Chief of Staff Rear Admiral Piyal De Silva stated that 'The Sri Lanka Navy has strengthened its presence; both inside and outside the Hambantota Port'[77] and further the former Chief of Staff declared that Sri Lanka Navy ensures the ISPS Code is properly implemented inside the port and if there is any security threat determined, Sri Lanka Navy would take prompt preventive measures against the threat.[78]

[76] Bergqvist (n 9).
[77] Rutnam Easwaran, 'Navy strengthens presence in and around Hambantota Port' (The Sunday morning, 21 October 2018) <http://www.themorning.lk/hambantota/> accessed 24 November 2020.
[78] ibid.

Sri Lankan Harbours Operate Under the ISPS Code



It was discussed earlier that MSC had promulgated guidance on implementing National Maritime Security Legislation in 2016 for SOLAS Contracting Governments. Since there is an international framework that has been established to implement maritime security measures in National Legislations and now the task is up to the Governments to make it a reality. When implementing legislation, the freedom has given to include all appropriate measures in accordance with the apparent local needs.[79] Therefore as well as the other states in the region, Sri Lanka too can initiate action to lay the foundation for a legislation to implement the ISPS Code, and it is not just a mere responsibility.

Since certain provisions of the ISPS Code are already enforced in Sri Lanka, one might argue that it would be sufficient and there is no requirement to draft a National Legislation. But, if Sri Lanka possesses a National Legislation drafted on the ISPS Code according to the local needs, it would be more efficient for international trade as well as for the enhancement of the security in Sri Lankan ports.

7. Incorporation and Implementation of the ISPS Code into Sri Lankan Legal System

When read Article 27(15) of the 1978 Constitution of the Democratic Socialist Republic of Sri Lanka with Article 154(G) (11), it is observed that since Sri Lanka is a dualist country; it is required to incorporate international instruments to the domestic legal system through national legislations. Therefore, an international instrument comes into operation to local legislation after a lengthy legislative process. The ISPS Code is the amendment brought to Chapter XI-2 of the SOLAS Convention and it is one of the most important international maritime conventions which Sri Lanka has been ratified so far and it came into operation with effect from 1 July 2016.[80]

Sri Lanka is a member of IMO and therefore, obligated to act according to the accords related to international maritime transport promulgated by the IMO. The Merchant Shipping Secretariat, a subsidiary of the Ministry of Ports and Shipping, is the Shipping Administration of Sri Lanka and functions as Sri Lanka's hub in the United Nations (UN) and IMO as well as overall responsibility for overseeing maritime concerns. Implementation of SOLAS Convention in Sri Lanka had been commenced to increase the security of container ships, maintain the stability and balance of ships, storing containers properly and minimizing the environmental impact.

The activities of the Merchant Shipping Secretariat are basically governed by the Merchant Shipping Act No.52 of 1971 as amended by No 17 of 2019, Licensing of Shipping Agents Act No. 10 of 1972 and also the relevant clauses of the Admiralty Jurisdiction Act No. 40 of 1983 and subsequent Regulations made thereafter. Merchant Shipping Secretariat deals with ensuring the

[79] IMO (n 7).

[80] Daily FT, 'Port & Shipping Ministry to host SOLAS convention' (Daily FT, 15 June 2016) < http://www.ft.lk/News/port-shipping-ministry-to-host-solas-convention/56-548397> accessed 10 January 2021.

safety of life and property at sea, maritime education, training, examination and certification, registration of ships under Sri Lanka flag, licensing of shipping agents, container depot operators, container terminal operators, container freight stations, freight forwarders or a non-vessel operating common carriers and implementing provisions of all applicable international maritime conventions, national regulations and it has developed and implemented maritime safety policy too.[81]

As it is discussed earlier, to incorporate any international instrument into the domestic legal system, it generally initiates through the Legislature, the Parliament of Sri Lanka. However, there are some instances where the relevant Minister is empowered by the Legislation to promulgate relevant Regulations by virtue of the powers vested in him on behalf of the Legislature. In such instances the relevant Minister may promulgate Regulations though Gazette notifications. According to Section 321(1) (i) of the Merchant Shipping Act No.52 of 1971 as amended by No 17 of 2019, the relevant Minister may make Regulations in respect of enforcement of any international convention in relating to the subject-matters of this Act and generally to all maritime matters.

Accordingly, the Minister of Ports and Shipping is empowered to enforce the proposed Regulations to the ISPS Code. As per section 321 (2), the Regulations shall come into operation on the date of such publication of the Gazette notification or on such later date as may be specified in the Regulation. Further section 321 (3) illustrated the Regulations made by the Minister shall, as soon as convenient after its publication in the Gazette, be brought before the parliament for approval. Any Regulation which is not so approved shall be deemed to be rescinded as from the date of such disapproval, but without prejudice to anything previously done thereunder.

When deciding the penalties, the Minister has to refer Chapter 2, Section 287 of the Merchant Shipping Act No 52 of 1971 as amended by No 17 of 2019. Accordingly, the jurisdiction for the offences which come under this Act vested with the Magistrate Court. Under section 30 of the Judicature Act No 2 of 1978, Magistrate's Court is vested with original criminal jurisdiction. Further as per Section 55(2) (b) 'Magistrate's Court-fine not exceeding one thousand five hundred rupees or imprisonment either simple or rigorous, for a period not exceeding eighteen months' unless, power is vested in the Magistrate's Court to impose higher penalties by special provision.

As per Regulation 6 of the proposed Regulation, any person who acts in contravene to a provision of these Regulations is committing an offence, and upon a conviction that person is liable to a fine not exceeding Rs.500,000.00 or imprisonment for a term not exceeding 02 years. This is proposed in consonance with the fines prescribed in the Fisheries (Regulation of Foreign Fishing Boats) (Amendment) Act, No. 1 of 2018 in proportionate to the present context. Jurisdiction is vested with the Magistrate Court under the aforementioned Act and for this proposed Regulation

[81] Director General Merchant Shipping, 'Ministry of Ports and Shipping, Merchant Shipping Secretariat'< http://www.dgshipping.gov.lk/web/index.php?lang=en> accessed 10 January 2021.

also it is possible to apply the same jurisdiction under Section 287 of the Merchant Shipping Act No 52 of 1971 as amended by No 17 of 2019.

8. Explanation on Textual Content of the Proposed Regulation

The text of the proposed Regulation consists of thirty-two Regulations and five Schedules. Therefore, the provisions in part 'A' and 'B' of the 2003 and 2012 editions of the ISPS Code have been considered for preparing the proposed Regulation. As per the ISPS Code, the prime objective is 'to enhance cooperation between governments, 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 facility used in international trade'. Hence this draft Regulation would cover the extent of the security levels the Sri Lankan Ports facilities and the Merchant Ships are arriving in Sri Lanka should adhere to.

The proposed Regulation basically discussed objectives, interpretation and the application in the very first Regulations. Subsequently, the Regulation discussed responsibilities of the Designated Authority, responsibilities of shipping companies and ships, Recognized Security Organization, port facilities and the certification of ships. Here onwards, it is discussed briefly some important provisions stated above.

(a) Objectives, Interpretation and the Application

The objectives and the application mentioned in this Regulation are almost similar to the ISPS Code. But in the Interpretation clause in the Regulation 3 unlike in the Code, the Authority has been vested with two Government Agencies. That is Merchant Shipping Secretariat of Sri Lanka acts as the 'Authority' and powers were delegated to Sri Lanka Navy to act as 'Designated Authority' as discussed earlier. Another significant interpretation is the 'PFSO' and this officer is appointed by the Commander of Navy to liaise with respective area commanders to perform duties as PFSOs and those officers are responsible for the development, implementation, revision and maintenance of the PFSP and also to liaise with the SSOs and CSOs. 'Contracting Government' in connection with any reference to a port facility, when used in this Regulations 20 to 24 and 27 includes a reference to the Designated Authority.

All the terms have been defined under the provisions of the Merchant Shipping Act No 52 of 1971 as amended by No 17 of 2019, SOLAS Convention on 1974 as amended which Sri Lanka is a State Party and the ISPS Code.

(b) Responsibilities of the Designated Authority

The responsibilities of the Designated Authority and also the responsibility in relation to the Declaration of Security have been discussed in Regulation 7 and 8.

(c) Responsibilities of Shipping Companies and Ships

This is discussed in Regulation 9 to Regulation 18 under the obligations of companies, ship security, SSA, SSP, CSO, SSO and training, drills and exercise on ship security.

(d) Recognized Security Organization

The Contracting Government; the Government of Sri Lanka has the discretion to nominate RSO and delegate powers to Designated Authority as well as to RSO. If RSO has appointed, the requirements for a RSO is set in Regulation 19.

(e) Port Facilities

Under this section, the Regulation deals with port facility security, PFSA, PFSP, PFSO, Port security committee, Port security personnel, training drills and exercises on port facility security and other related matters from Regulation 20 to 27. In this Regulation it is proposed a Port security committee and the Port security personnel, unlike in the Code and it is included a naval officer as ISPS Officer to the Port security committee. Sri Lanka Navy has already appointed officers as ISPS Officers for the seven harbours where the Code is functioning in Sri Lanka at present.

(f) Certification of Ships

In the proposed Regulation from Regulation 28 to Regulation 31 it is discussed verification and certification for ships, issue and endorsement of certificates and interim certification.

(g) Sinhala Text to Prevail in case of Inconsistency

Article 23 (1) of the 1978 Constitution of Sri Lanka provides that all laws, and subordinate legislation shall be enacted or made and published in Sinhala and Tamil together with a translation thereof in English. According to Article 18 (1) and (2) of the Constitution, Sinhala and Tamil are recognized as Official State Languages. Thereby, Regulation 32 of the proposed Regulation has been drafted capturing the wordings to the effect ‘in the event of any inconsistency between the Sinhala and Tamil texts, the Sinhala text of this Act shall prevail’.

The Gazette of the Democratic Socialist Republic of Sri Lanka

Government Notifications

THE MERCHANT SHIPPING ACT, NO.52 OF 1971

Merchant Shipping (International Ship and Port Facility Security Code) Regulations, 2021

REGULATIONS made by the Minister of Ports and Shipping by virtue of the powers vested in him by section 321 of the Merchant Shipping Act, No.52 of 1971

Rohitha Abeygunawardena

Minister of Ports and Shipping

In Colombo,

…..day of …. 2021

Regulations

Title

1. These Regulations may be cited as the Merchant Shipping (International Ship and Port Facility Security Code) Regulations, 2021 and shall come into operation with effect from.....

Objectives

2. (1) The objectives of these Regulations are to establish a National framework amongst Government Agencies, the Authority and the Shipping and Port Industry to detect, access and take preventative measures against any security threat or incident affecting ships or port facilities in Sri Lanka used in international trade.

(2) These Regulations prescribe:

(a) establish the respective roles and responsibilities of all parties concerned for ensuring maritime security, and the early and efficient collation and exchange of security related information; and

(b) provide the methodology for security assessments for plans and procedures to counter changing security levels in Sri Lanka.

Interpretation

3. (1) In these Regulations, unless the context otherwise requires:

'**Administration**' means the government of the State whose flag the ship is entitled to fly;

'**Authority'**' means Merchant Shipping Secretariat of Sri Lanka who is responsible for the implementation of these Regulations;

'**Chapter**' means a chapter of the Convention;

'**Code**' means the International Ship and Port Facility Security (ISPS) Code adopted on 12 December 2002 by resolution 2 of the Conference of Contracting Governments to the

International Convention for the Safety of Life at Sea, 1974 (SOLAS), as may be amended by the International Maritime Organization:

'**Company**' means the owner of the ship and includes a person, manager or the bareboat charterer, who has assumed the responsibility for the operation of the ship from the ship owner as imposed by these Regulations and the Code;

'**Company Security Officer**' means a person designated by a Company for ensuring that a ship security assessment is carried out and the Ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with the Port Facility Security Officers and the Ship Security Officer;

'**Convention**' means the International Convention for the Safety of Life at Sea (SOLAS) 1974, as adopted by the International Conference on Safety of Life at Sea on 01 November 1974, which entered into force on 25 May 1980, as amended from time to time;

'**Declaration of Security**' means an agreement, made in the format appended in Schedule 1, between a ship and a port facility or another ship which specifies the security measures each will implement;

'Designated Authority' means Sri Lanka Navy to undertake security duties relating to Port facilities as set out in Chapter XI-2 of the Convention

'**Mobile offshore drilling unit**' means a mechanically propelled mobile offshore drilling unit, as defined in Chapter IX- 1 of the Convention;

'**Port facility**' means a location, as determined by the Authority, where ship or port interface takes place and includes areas such as anchorage, awaiting berths and approaches from seaward;

'**Port Facility Security Officer**' means the respective Officers of Sri Lanka Navy appointed by the Commander of Navy to perform duties as Port Facility Security Officer and this Officer is 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;

'**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;

'**Recognized Security Organization**' means a Recognized Security Organization with expertise in security matters and with appropriate knowledge of ships and port operations authorized to carry out an assessment or verification or approval or certification required by these Regulations and the Code;

'**Security incident**' means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a Port facility or of any ship or port interface or any Ship to ship activity;

'**Security level**' means the qualification of the degree of risk that a Security incident will be attempted or will occur;

'**Security level 1**' means the normal level of security at which the ship or Port facility normally operates with minimum appropriate protective security measures;

'**Security level 2**' means the heightened level of security applying for as long as there is a heightened risk of a Security incident for which appropriate additional protective security measures shall be maintained;

'**Security level 3**' means the exceptional level of security applying for the period of time when there is the probable or imminent risk of a security incident for which further specific protective security measures shall be maintained;

'**Ship Security Officer**' means the Ship Security Officer on board the ship, accountable to the Master, designated by the Company as responsible for the security of the ship, implementation and maintenance of the ship security plan and for liaison with the Company Security Officer and the Port Facility Security Officer;

‘**Ship security plan**’ means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident;

‘**Ship to ship activity**’ means any activity not related to a Port facility that involves the transfer of goods or persons from one ship to another.

(2) The term "**ship**", when used in these Regulations and the Code, includes mobile offshore drilling units and high-speed craft as defined in Chapter XI- 2/ l.

(3) The term "**Contracting Government**" in connection with any reference to a port facility, when used in this Regulations 20 to 24 and 27, includes a reference to the Designated Authority.

(4) The words and terms not otherwise defined in these Regulations shall have the same meaning as the meaning attributed to them in chapters 1 and XI- 2 of the Convention.

Application

4. (1) These Regulations apply to:

(a) 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 upwards;

(iii) mobile offshore drilling units; and

(b) port facilities serving such ships engaged in international voyages.

(2) These Regulations do not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial services.

(3) Notwithstanding sub-regulation (1), the Authority shall decide the extent of application of these Regulations to Port facilities within Sri Lanka which, although used primarily by ships not

engaged in international voyages, which are also required, occasionally, to serve ships arriving or departing on an international voyage.

(4) The Designated Authority shall base its decision on a port facility security assessment carried out in accordance with these Regulations.

(5) No decision of the Designated Authority shall compromise the level of security intended to be achieved by Chapter XI-2 of the Convention or by these Regulations.

(6) Regulations 8 to 18 and 28 to 31 shall apply to Companies and ships as specified in Chapter XI-2/4.

(7) Regulations 8 and 20 to 27 shall apply to port facilities as specified in Chapter XI-2/l0.

(8) Nothing in these Regulations shall prejudice the rights or obligations of the Democratic Socialist Republic of Sri Lanka under international law.

Certificate of Compliance

5. (1) The Authority may, upon application and after assessing and verifying a ship, port or Port facility under Article 3 of the Code, issue a Certificate of Compliance to the ship, port or Port facility in the form prescribed under Schedule 2.

(2) The applicant for a certificate of compliance shall pay the fees to the Authority as prescribed in Schedule 3.

Offences and Penalties

6. Any person or owner, operator or agent of a ship, port or Port facility to which the Code applies that contravenes a provision of these Regulations commits an offence and is upon conviction liable to a fine not exceeding [**Rs. 500,000.00 or imprisonment for a term not exceeding 02 years**].[82]

[82] In consonance with the fines prescribed in the Fisheries (Regulation of Foreign Fishing Boats) (Amendment) Act, No. 1 of 2018.

Responsibilities of the Designated Authority

7. (1) Subject to the provisions of Chapters XI-2/3 and XI-2/7 of the Convention, the Designated Authority shall set Security levels and issue guidelines for protection from Security incidents.

(2) The higher security levels indicate a greater likelihood of occurrence of a security incident and the Designated Authority shall, *inter alia*, consider the following factors while setting the appropriate Security level:

(a) the degree that the threat information is credible;

(b) the degree that the threat information is corroborated;

(c) the degree that the threat information is specific or imminent; and

(d) the potential consequences of such a Security incident.

(3) The Designated Authority, while setting Security level 3, shall issue appropriate instructions and provide security related information to the ships and Port facilities that are likely to be affected.

(4) The Designated Authority may delegate to a Recognized Security Organization certain responsibilities under Chapter XI-2 of the Convention and these Regulations, except the powers of:

(a) setting of the Security levels;

(b) approving a port facility security assessment and any amendment to the approved assessment;

(c) determining the Port facilities which will be required to designate a Port Facility Security Officer;

(d) approving a Port facility Security Plan and any subsequent amendment to an approved plan;

(e) exercising control and compliance measures pursuant to Chapter XI-2/9 of the Convention; and

(f) establishing the requirements for a Declaration of Security.

(5) The Designated Authority shall, to the extent it considers appropriate, test the effectiveness of the ship or the Port facility Security Plans, or any amendments to such plans it has approved or in the case of a ships, of Ships security plans which have been approved on its behalf.

Declaration of Security

8. (1) The Designated Authority shall determine when a Declaration of Security is required under sub-regulation (2) by assessing the risk the ship and port interface or Ship to ship activity poses to persons, property or the environment.

(2) A ship may request completion of a Declaration of Security when:

(a) the ship is operating at a higher Security level than the Port facility or another ship it is interfacing with;

(b) there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;

(c) there has been a security threat or a Security incident involving the ship or involving the Port facility, as applicable;

(d) the ship is at a port which is not required to have and implement an approved Port facility Security Plan; or

(e) the ship is conducting ship to ship activities with another ship not required to have and implement an approved Ship security plan.

(3) The requests for the completion of a Declaration of Security under sub-regulation (2) shall be acknowledged by the Port facility or ship.

(4) The Declaration of Security shall be completed by:

(a) the Master or the Ship Security Officer on behalf of the ship; and

(b) the Port Facility Security Officer or, if the Designated Authority determines otherwise, by any other person responsible for shore-side security, on behalf of the Port facility.

(5) The Declaration of Security shall address the security requirements that could be shared between a Port facility and a ship and shall state the responsibility of each.

(6) The Designated Authority shall, subject to the provisions of Chapter XI-2/9.2.3 of the Convention, specify the minimum period for which Declarations of Security shall be kept by the Port facilities located within Sri Lanka.

(7) The Designated Authority shall, subject to the provisions of Chapter XI-2/9.2.3 of the Convention, specify the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

Obligations of the Company

9. (1) The Company shall ensure that the Ship security plan contains a clear statement emphasizing the Master's authority.

(2) The Company shall establish in the Ship security plan that the Master has the overriding authority and power to make decision with respect to the safety and security of the ship and to request the assistance of the Company or the Designated Authority as may be necessary.

(3) 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 Chapter XI-2 of the Convention and these Regulations.

Ship Security

10. (1) A ship is required to act upon the Security levels set by the Administration and the Security levels set in sub-regulations (2), (3) and (4).

(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 the Code, in order to identify and take preventive measures against security incidents:

(a) ensuring the performance of all ship security duties;

(b) controlling access to the ship;

(c) controlling the embarkation of persons and their effects;

(d) monitoring restricted areas to ensure that only authorized persons have access;

(e) monitoring of deck areas and areas surrounding the ship;

(f) supervising the handling of cargo and ship's stores;

(g) ensuring that security communication is readily available; and

(h) ensure liaison with the Port facility to ensure designated secure area for inspection and searching of persons, baggage, personal effects, vehicles and contents can take place while embarking or disembarking the ship

(3) At Security level 2, the additional protective measures, specified in the Ship security plan, shall be implemented for each activity detailed in sub-regulation (2), which may include the following elements:

(a) deploying additional personnel to patrol deck areas during silent hours to deter unauthorized access;

(b) limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;

(c) deterring waterside access to the ship, including for example, in liaison with the Port facility, provision of boat patrols;

(d) establishing a restricted area on the shore-side of the ship, in close cooperation with the Port facility;

(e) increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;

(f) escorting visitors on the ship;

(g) providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance; and

(h) carrying out a full or partial search of the ship.

(4) At Security level 3, further specific protective measures, specified in the Ship security plan, shall be implemented for each activity detailed in sub-regulation (2), which may include the following elements:

(a) limiting access to a single, controlled, access point;

(b) granting access only to those responding to the security incident or threat thereof;

(c) directions of persons on board;

(d) suspension of embarkation or disembarkation;

(e) suspension of cargo handling operations and deliveries;

(f) evacuation of the ship;

(g) movement of the ship; and

(h) preparing for a full or partial search of the ship.

(5) Whenever Security level 2 or Security level 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the Security level.

(6) A ship shall, prior to entering a port in Sri Lanka or whilst in a port in Sri Lanka that has set Security level 2 or Security level 3:

(a) acknowledge the receipt of instructions as required under sub-regulation (5);

(b) 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, and in the case of Security level 3, instructions issued by the Designated Authority which has set Security level 3; and

(c) report to the Designated Authority any difficulties in implementation, and in such case, the Port Facility Security Officer and Ship Security Officer shall liaise and co-ordinate the appropriate actions.

(7) If a ship is required by the Administration to set, or is already at, a higher Security level than that set for any port in Sri Lanka it intends to enter or in which it is already located, then the ship shall advise, without delay, to the Designated Authority of the situation and in such case, the Ship Security Officer shall liaise with the Port Facility Security Officer and co-ordinate appropriate actions, if necessary.

(8) When the Administration requires ships entitled to fly its flag to set Security level 2 or Security level 3 in a port of another Contracting Government, the Administration shall inform that Contracting Government without delay.

(9) When the Designated Authority sets Security levels and ensures the provision of Security level information to ships operating in Sri Lankan waters, or the ship has communicated its intention to enter into Sri Lankan waters, such ships shall be advised to maintain vigilance and report immediately to the Designated Authority and any nearby Coastal States, any information that comes to their attention that might affect maritime security in the area.

(10) The Designated Authority, when advising such ships of the applicable Security level, shall advise those ships of any security measures that they should take and, if appropriate, of measures that have been taken by the Designated Authority to provide protection against the threat.

Master's Discretion

11. (1) The Master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgment of the Master, is necessary to maintain the safety and security of the ship. This may include denial of access to persons, except those authorized by the Authority or their effects and refusal to load cargo, including containers or other closed cargo transport units.

(2) If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the Master may give precedence to measures intended to maintain the safety of the ship, and take such temporary security measures as seem best under all circumstances.

Ship Security Assessment

12. (1) The ship security assessment is an essential and integral part of the process of developing and updating the Ship security plan.

(2) The Company Security Officer shall ensure that the ship security assessment is carried out by persons having appropriate skills to evaluate the security of a ship, in accordance with this regulation, taking into account the guidance given in Part B of the Code.

(3) Subject to sub-regulation (2), a Recognized Security Organization may carry out the ship security assessment of a specific ship.

(4) The ship security assessment shall include an on scene security survey and, at least, the following elements:

(a) identification of existing security measures, procedures and operations;

(b) identification and evaluation of key ship board operations that it is important to protect;

(c) identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and

(d) identification of weaknesses, including human factors in the infrastructure, policies and procedures.

(5) The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

Ship Security Plan

13. (1) Sri Lankan ships on international voyages shall carry on board a Ship security plan approved by the Government of Sri Lanka, which shall make provisions for three Security levels as defined in these Regulations.

(2) Subject to Regulation 12(2), a Recognized Security Organization may prepare the Ship security plan for a specific ship.

(3) The Government of Sri Lanka may entrust the review and approval of Ship security plans, or any amendment to a previously approved plan, to the Recognized Security Organization.

(4) The Recognized Security Organization who has been involved in the preparation of the ship security assessment or the Ship security plan or any amendment thereto shall not undertake the review and approval of a Ship security plan, or its amendment on behalf of the Government of Sri Lanka for a specific ship.

(5) The submission of a Ship security plan or of amendment to a previously approved plan for approval shall be accompanied by the security assessment on the basis of which the plan or the amendment has been developed.

(6) The plan shall be developed, taking into consideration the guidance given in Part B of the Code and written in the working language or languages of the ship, and if the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included, and the plan shall address, at least, the following:

(a) 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;

(b) identification of the restricted areas and measures for the prevention of unauthorized access;

(c) measures for the prevention of unauthorized access to the ship;

(d) procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship and port interface;

(e) procedures for responding to any security instructions which may be issued by the Administration for Security level 3;

(f) procedures for evacuation in case of security threats or breaches of security;

(g) duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

(h) procedures for auditing the security activities;

(i) procedures for training, drills and exercises associated with the plan;

(j) procedures for interfacing with Port facility security activities;

(k) procedures for the periodic review of the plan and for updating;

(l) procedures for reporting Security incidents;

(m) identification of the Ship Security Officer;

(n) identification of the Company Security Officer including 24-hour contact details;

(o) procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

(p) frequency for testing or calibration of any security equipment provided on board;

(q) identification of the locations where the ship security alert system activation points are provided; and

(r) 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.

(7) Every 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 it is impracticable due to the size and the nature of the Company or of the ship.

(8) The Designated Authority shall determine which changes to an approved Ship security plan or to any security equipment specified in an approved plan shall not be implemented unless

the relevant amendments to the plan are approved by the Administration, and any such changes shall be at least as effective as those measures prescribed in Chapter XI-2 of the Convention and these Regulations.

(9) The nature of the changes to the Ship security plan or the security equipment that have been specifically approved by the Administration, shall be documented in such manner that clearly indicates such approval and be available on board, and be presented together with the International Ship Security Certificate. In case the changes are temporary, once the original approved measures or equipment is reinstated, the documentation under this sub-regulation no longer needs to be retained by the ship.

(10) 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.

(11) The plan shall be protected from unauthorized access or disclosure.

(12) The Ship security plan is not subject to inspection by the Port State Control Officer, except in the circumstances specified in sub-regulation (13).

(13) If the Port State Control Officer authorized by the Government of Sri Lanka has reasonable grounds to believe that the ship is not in compliance with the requirements of Chapter XI-2 of the Convention or Part A of the Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the Ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government or the Master of the ship concerned.

(14) Notwithstanding anything in sub-regulation (13), the provisions in the plan relating to sub-regulation (6) (b), (d), (e), (g), (o), (q) and (r) are confidential information and shall not be subjected to inspection unless otherwise agreed to by the Administration concerned.

Maintenance of Records

14. (1) The records of ship's security activities mentioned in the Ship security plan, including Declarations of Security and the record of the ship security level shall be maintained on board for a period covering at least the previous 10 calls at port facilities or a period specified by the

Administration keeping in view the following provisions of Chapter XI-2/9.2.3 of the Convention, namely:

(a) training, drills and exercises;

(b) security threats and Security incidents;

(c) breaches of security;

(d) changes in Security level;

(e) 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;

(f) internal audits and reviews of security activities;

(g) periodic review of the ship security assessment;

(h) periodic review of the Ship security plan;

(i) implementation of any amendments to the plan; and

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

(2) The records shall be kept in the working language or languages of the ship, and if the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

(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.

(4) The records shall be protected from unauthorized access or disclosure.

Audit of Ship Security Plan

15. The Ship security plan shall be audited at intervals not exceeding 5 years, and the plan shall be verified annually for compliance by the Government of Sri Lanka or the Recognized Security Organization.

Company Security Officer

16. (1) The Company shall designate a Company Security Officer, who may act as the Company Security Officer for one or more ships, depending on the number or types of ships the Company operates, provided it is clearly identified for which ships that person is responsible.

(2) 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.

(3) Every Company shall appoint a Company Security Officer to implement and administer the requirements of these Regulations.

(4) The Company Security Officer shall be empowered to:

(a) enter ships to make inquiries, examinations, inspections and searches in accordance with this regulation; and

(b) implement all security measures as required by this Regulation.

(5) In addition to those specified elsewhere in these Regulations, the duties and responsibilities of the Company Security Officer shall include, but are not limited to:

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

(b) ensuring that ship security assessments are carried out;

(e) ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the Ship security plan;

(d) ensuring that the Ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

(e) arranging for internal audits and reviews of security activities;

(f) arranging for the initial and subsequent verifications of the ship by the Designated Authority or the approved Recognized Security Organization;

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

(h) enhancing security awareness and vigilance;

(i) ensuring adequate training for personnel responsible for the security of the ship;

(j) ensuring effective communication and co-operation between the Ship Security Officer and the relevant Port Facility Security Officers;

(k) ensuring consistency between security requirements and safety requirements;

(I) ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately;

(m) ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships arc implemented and maintained;

(n) ensuring the conduct of ship security drills and exercises;

(0) ensuring the proper maintenance of all records pertaining to the ship's security;

(p) notifying law enforcement agencies and other law enforcement respondents of ship Security incidents and any breaches of these Regulations; and

(q) ensuring that all security measures set forth in this regulation arc implemented and enforced.

Ship Security Officer

17. (1) Companies shall appoint a designated Ship Security Officer aboard each security regulated ship to implement and administer the requirements of this Regulation.

(2) The Ship Security Officer shall be empowered to:

(a) implement various levels of physical security controls aboard assigned security regulated ships; and

(b) implement security measures as required by this Regulation.

(3) In addition to those specified elsewhere in these Regulations, the duties and responsibilities of the Ship Security Officer shall include, but are not limited to:

(a) undertaking regular security inspections of the ship to ensure that appropriate security measures arc maintained;

(b) maintaining and supervising the implementation of the Ship security plan, including any amendments to the plan;

(c) coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant Port Facility Security Officers;

(d) proposing modifications to the Ship security plan;

(e) 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;

(f) enhancing security awareness and vigilance on board;

(g) ensuring that adequate training has been provided to shipboard personnel, as appropriate;

(h) reporting all Security incidents;

(i) coordinating implementation of the Ship security plan with the Company Security Officer and the relevant Port Facility Security Officer;

(j) ensuring that security equipment is properly operated, tested, calibrate and maintained, if any;

(k) ensuring the conduct of ship security drills and exercises;

(l) ensuring the proper maintenance of all records pertaining to the ship's security;

(m) notifying the Company Security Officer or in the absence of a Company Security Officer to the law enforcement agencies and other law enforcement

respondents, of ship security incidents and any breaches of any provisions of these Regulations; and

(n) ensuring that all security measures set forth in this Regulation are implemented and enforced.

Training, Drills and Exercise on Ship Security

18. (1) A person shall not be appointed as the Company Security Officer or the Ship Security Officer unless such person has the knowledge and training in the following areas:

(a) security administration;

(b) relevant international conventions, codes and recommendations;

(c) relevant Government laws;

(d) responsibilities and functions of other security organizations;

(e) ship's security assessment;

(f) ship security surveys and inspections;

(g) ship and port facility security measures;

(h) emergency preparedness and response and contingency planning;

(i) security measures and procedures;

(j) classification of security information;

(k) recognition of security threats and patterns;

(l) overview of International Ship and Port facility Security audits;

(m) methods of physical searches and non-intrusive inspections;

(n) security drills and exercises, including drills and exercises with Port facilities; and

(o) assessment of security drills and exercises.

(2) Every shipboard personnel delegated any duty under the Ship security plan shall have sufficient knowledge and ability to perform the assigned duties.

(3) In order to ensure the effective implementation of the Ship security plan, drills shall be carried out at least every three months.

(4) When 25% of ship's personnel have been changed, with personnel that have not previously participated in any drill on that ship within the last three months, a drill must be conducted within one week of this change, and these drills should test individual elements of the plan.

(5) The Company Security Officer may participate in the security exercises in conjunction with relevant Administration, Ship Security Officer if available, and Port Facility Security Officer, once each calendar year with not more than 18 months intervals in between, to ensure the effective coordination and implementation of Ship security plans.

(6) These drills and exercises shall test communications, coordination, resource availability and response may be:

(a) a full scale or live exercise;

(b) a table-top simulation; or

(c) a combined with search and rescue or emergency response exercise.

Recognized Security Organization

19. (1) The Government of Sri Lanka may authorize a Recognized Security Organization to undertake certain security related activities on behalf of the State, consisting of the following:

(a) conduct security assessments;

(b) inspect and audit port facilities;

(c) advise or provide assistance on security matters.

(2) Notwithstanding anything in sub-regulation (1), the Recognized Security Organization shall not:

(a) set Security levels;

(b) approval of Security assessments;

(c) approval of Security plans; or

(d) exercise ship control and compliance measures,

(3) The Designated Authority shall ensure that the Recognized Security Organization has the necessary competencies to perform the duties authorized under sub-regulation (1), and considering the qualification of the Recognized Security Organization, the Designated Authority shall ensure that the Recognized Security Organization is able to demonstrate competence in the following areas:

(a) expertise in relevant aspects of security;

(b) appropriate knowledge of ship and port operations, including general knowledge of Recognized Security Organization ship's layout and port layout when providing services for such ships and Port facilities;

(c) capability to assess the likely security risks that could occur during ship and port facility operations, including the ship and port interface and the ways to minimize such risks;

(d) training and improving the expertise of their personnel;

(e) screening of their security personnel;

(f) security of documents and sensitive materials;

(g) application of the requirements of Chapter XI-2 of the Convention and these Regulations and relevant national and international laws and security requirements;

(h) knowledge of current security threats and patterns;

(i) ability to recognize and detect weapons, dangerous substances and devices;

(j) ability to recognize behavioural patterns of persons who are likely to threaten security;

(k) knowledge on techniques used to circumvent security measures; and

(l) knowledge of security and surveillance equipment and systems and their operational limitations.

(4) The Government of Sri Lanka may revoke the authorization of the Recognized Security Organization under sub-regulation (1), if the Recognized Security Organization fails to meet or maintain the conditions and qualifications specified in this Regulation.

Port Facility Security

20. (1) A Port facility in Sri Lanka is required to act upon the Security levels set by the Designated Authority and the 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.

(2) At Security level 1, the following activities shall be carried out through appropriate measures in all Port facilities, considering the guidance given in Part B of the Code, in order to identify and take preventive measures against security incidents:

(a) ensuring the performance of all port facility security duties;

(b) controlling access to the Port facility;

(c) monitoring of the Port facility, including anchoring and berthing areas;

(d) monitoring restricted areas to ensure that only authorized persons have access;

(e) supervising the handling of cargo;

(f) supervising the handling of ship's stores; and

(g) ensuring that security communication is readily available.

(3) At Security level 2, the additional protective measures specified in the Port facility Security Plan shall be implemented for each activity detailed in sub-regulation (2), considering the guidance given in Part B of the Code.

(4) At Security level 3, further specific protective measures specified in the Port facility Security Plan shall be implemented for each activity detailed in sub-regulation (2), Port facility Security considering the guidance given in Part B of the Code and in addition, at Security level 3, the Port facilities in Sri Lanka are required to respond to and implement any security instructions given by the Designated Authority.

(5) When a Port Facility Security Officer is advised that a ship encounters difficulty in complying with the requirements of Chapter XI-2 of the Convention or these Regulations 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 Designated Authority, the Port Facility Security Officer and Ship Security Officer shall liaise and co-ordinate appropriate actions.

(6) When a Port Facility Security Officer is advised that a 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 Designated Authority and shall liaise with the Ship Security Officer and co-ordinate appropriate actions, if necessary.

Port Facility Security Assessment

21. (1) The Port facility security assessment is an essential and integral part of the process of developing and updating the Port facility Security Plan.

(2) The Port facility security assessment shall be carried out by the Designated Authority, or the Designated Authority may authorize a Recognized Security Organization to carry out the Port facility security assessment of a specific Port facility in Sri Lanka.

(3) When the Port facility security assessment has been carried out by a Recognized Security Organization, the security assessment shall be reviewed and approved for compliance with this Regulation by the Designated Authority.

(4) The persons carrying out the assessment shall have appropriate skills to evaluate the security of the Port facility in accordance with this Regulation, considering the following elements:

(a) physical security;

(b) security equipment;

(c) security procedures;

(d) radio communications systems (including information technology systems and networks);

(e) transportation infrastructure;

(f) utilities infrastructure;

(g) other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port, port facility or aboard ships adjacent thereto; and

(h) available expert assistance.

(5) The Port facility security assessments shall be reviewed and updated, annually considering changing threats or minor changes in the Port facility and shall always be reviewed and updated when major changes to the Port facility take place.

(6) The Port facility security assessment shall include, at least, the following elements:

(a) identification and evaluation of important assets and infrastructure which are important to protect;

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

(c) identification, selection and prioritization of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability; and

(d) identification of weaknesses, including human factors in the infrastructure, policies and procedures;

(7) The Designated Authority may allow a Port facility security assessment to cover more than one Port facility if the operator, location, operation, equipment, and design of the Port facilities

are similar, and if the Designated Authority allows such an arrangement, it shall communicate to the International Maritime Organization the particulars thereof.

(8) Upon completion of the Port facility security assessment, a report shall be prepared, consisting of:

(a) a summary of how the assessment was conducted;

(b) a description of each vulnerability found during the assessment; and

(c) a description of counter-measures that could be used to address each vulnerability.

(9) The report referred to in sub-regulation (8) shall be protected from unauthorized access or disclosure.

Port Facility Security Plan

22. (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 and port interface, and the plan shall make provisions for the three security levels, as defined in this Regulation.

(2) Subject to Regulation 19(2), a Recognized Security Organization may prepare the Port facility Security Plan for a specific port facility.

(3) The Port facility Security Plan shall be approved by the Designated Authority.

(4) The Port facility Security Plan shall be developed taking into consideration the guidance given in Part B of the Code and shall be in the working language of the Port facility, and the plan shall address, at least, the following elements:

(a) 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 onboard a ship;

(b) measures designed to prevent unauthorized access to the Port facility, to ships moored at the facility, and to restricted areas of the facility;

(c) procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the Port facility or ship and port interface;

(d) procedures for responding to any security instructions which may be issued by the Designated Authority for Security level 3;

(e) procedures for evacuation in case of security threats or breaches of security;

(f) duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;

(g) procedures for interfacing with ship security activities;

(h) procedures for the periodic review, auditing and updating of the security plan;

(i) procedures for reporting security incidents;

(j) identification of the Port Facility Security Officer including 24-hour contact details;

(k) measures to ensure the security of the information contained in the plan;

(l) measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

(m) procedures for auditing the Port facility Security Plan;

(n) procedures for responding in case the ship security alert system of a ship at the Port facility has been activated; and

(o) 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.

(5) The 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.

(6) 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.

(7) The Designated Authority shall determine which changes to the Port facility Security Plan shall not be implemented unless the relevant amendments to the plan are approved by the Authority.

(8) The plan may be kept in an electronic format and in such case; it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

(9) The plan shall be protected from unauthorized access or disclosure.

(10) The Designated Authority may allow a Port facility Security Plan to cover more than one port facility if the operator, location, operation, equipment, and design of these Port facilities are similar and such an alternative arrangement shall be communicated to the International Maritime Organization by the Designated Authority.

Port Facility Security Officer

23. (1) The Designated Authority shall appoint respective Officers of Sri Lanka Navy as the Port facility Security Officers.

(2) A Port Facility Security Officer shall be designated for each Port facility and may be designated as the Port Facility Security Officer for one or more port facilities.

(3) The Port Facility Security Officer shall be empowered to:

(a) enter Port facilities or board ships to make inquiries, examinations, inspections, searches, seizures and apprehend in accordance with this Regulation;

(b) exercise control measures over ships within the port and to require Declarations of Security with those ships; and

(c) implement all security measures and protocols as required by this Regulation,

(4) The Port Facility Security Officer may delegate any or all of his powers and functions under this Regulation to qualified Security Officers under his command with the approval of the Commander of Navy.

(5) In addition to those specified elsewhere in the Regulations, the duties and responsibilities of the Port Facility Security Officer shall include, but are not limited to:

(a) conducting an initial comprehensive security survey of the Port facility considering the relevant Port facility security assessment;

(b) ensuring the completion and timely audit of required security assessments;

(c) ensuring the development, submission, implementation and timely audit of required security plans;

(d) implementing and exercising the Port facility Security Plan;

(e) undertaking regular security inspections of the Port facility to ensure the continuation of appropriate security measures;

(f) conducting port security drills and exercises and submitting report to the Designated Authority;

(g) maintaining all security records for a period of 5 years;

(h) recommending and incorporating, as appropriate, modifications to the Port facility Security Plan to correct deficiencies and to update the plan to consider ~~of~~ relevant changes to the Port facility;

(i) enhancing security awareness and vigilance of the Port facility personnel;

(j) ensuring adequate training has been provided to personnel responsible for the security of the Port facility;

(k) reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the Port facility;

(l) coordinating implementation of the Port facility Security Plan with the appropriate Company and the Ship Security Officers;

(m) coordinating with security services, as appropriate;

(n) ensuring that standards for personnel responsible for security of the Port facility are met;

(o) ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

(p) assisting the Ship Security Officers in confirming the identity of those seeking to board the ship when requested.

Port Security Committee

24. (1) The Port Facility Security Officer shall constitute a Port Security Committee, of not less than five members, having an interest in the security of the area, who may be selected from:

(a) ISPS Officer appointed by the Designated Authority

(b) law enforcement and emergency response agencies;

(c) maritime industry; and

(d) other port stakeholders having a special competence in maritime security.

(2) The Port Security Committee shall:

(a) identify critical port infrastructure and operations;

(b) identify risks (threats, vulnerabilities, and consequences);

(c) determine mitigation strategies and implementation methods; and

(d) advise and assist the Port facility Security Officer in developing the security assessment and security plan.

(3) The Port Security Committee shall be empowered to:

(a) enter port and Port facility premises;

(b) inspect port and Port facility documents, records and plans;

(c) inspect port and Port facility security equipment; and

(d) assist with the planning and execution of port and Port facility security exercises.

Security Personnel

25. (1) Every port, Port facility, Shipping Company, ships and security personnel of the Recognized Security Organization shall be subjected to a background records check and police clearance requirements.

(2) Security assessment and Security plans audits shall be conducted by the Designated Authority or an organization approved by the Designated Authority that is independent of the Port facility subject to the assessment or audit.

Training Drills and Exercises on Port Facility Security

26. (1) The Port Facility Security Officer and appropriate port facility security personnel shall have sufficient knowledge, in basic ship and port security and the International Ship and Port Facility Security Code implementation and administration.

(2) The Port Facility Security Officer and Port facility security 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 training in the following areas:

(a) relevant provisions of the port, Port facility and Ship security plan;

(b) the relevance and application of Security levels;

(c) emergency procedures;

(d) recognition and detection of dangerous substances and devices;

(e) recognition of characteristics and behavioural patterns of persons who are likely to threaten security; and

(f) other training specific to their duties.

(3) In order to ensure the effective implementation of the Port facility Security Plan, drills shall be carried out at least once every 3 months to test all the individual elements of the port

facility security plan and the drills shall consider the specific threats and responses identified in the security assessment and the security plan and should test individual elements of the plan.

(4) The Designated Authority shall ensure that the Port Facility Security Officer carries out the security exercises once each calendar year with not more than 18 months between two exercises to test the effectiveness of the Port facility Security Plan, and enable the Security Officer to identify any security related deficiencies that need to be addressed.

(5) The security exercises may be:

(a) full scale or live;

(b) table-top simulation or seminar; or

(c) combined with other exercises.

Records, Audits, Review and Amendments

27. (1) The Port Facility Security Officer shall maintain all security records for a period of 5 years.

(2) The Port facility Security Plan shall be audited internally by the Port Facility Security Officer and externally by external auditors approved by the Government of Sri Lanka or by the Designated Authority auditors' at intervals not exceeding 5 years.

(3) The Port facility Security Plan shall be verified annually by the Designated Authority or approved Recognized Security Organization.

(4) The Port facility Security Plan shall be reviewed and updated or amended according to the procedures in the Port facility Security Plan by the Port Facility Security Officer, and it should be reviewed:

(a) if the Port facility security assessment relating to the Port facility is altered;

(b) if the external audit carried out by the Designated Authority or approved Recognized Security Organization identifies failings or outdated procedures in Port facility Security Plan;

(c) following Security incidents or threats thereof involving the Port facility; and

(d) following changes in ownership or operational control of the Port facility.

(5) The Port Facility Security Officer may recommend appropriate amendments to the approved plan following any review of the plan relating to:

(a) proposed changes to security measures of the Port facility; and

(b) the removal, alteration or replacement of any equipment and systems essential for maintaining the security of the Port facility.

(6) The amendments referred to in sub-regulation (5) shall be submitted to the Designated Authority for approval.

Verification and Certification for Ships

28. (1) Every ship to which these Regulations apply shall be subject to the following verifications, namely:

(a) an initial verification before the ship is put in service or before the certificate required under sub-regulation (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 Chapter XI-2 of the Convention, these Regulations and the approved Ship security plan, in order to ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 of the Convention and these Regulations, and is in satisfactory condition and fit for the service for which the ship is intended;

(b) a renewal verification at intervals specified by the Authority, but not exceeding 5 years, except where Regulation 22(4) applies to ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 of the Convention, these Regulations and the approved ship security verification for certification of ships plan, and is in satisfactory condition and fit for the service for which the ship is intended;

(c) an intermediate verification to be carried out between the second and third anniversary date of the certificate, which 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 and the intermediate verification shall be endorsed on the certificate; and

(d) any additional verifications as determined by the Authority.

(2) The verifications of ships shall be carried out by the Authority, or the Authority may entrust the verifications to a Recognized Security Organization referred to in Chapter XI-2/1 of the Convention.

(3) In every case, the Authority shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

(4) The security system and any associated security equipment of the ship after verification shall be maintained to conform to the provisions of Chapter XI-2/4.2 and Chapter XI-2/6 of the Convention, these Regulations and the approved Ship security plan.

(5) After any verification under sub-regulation (1) has been completed, no changes shall be made in security system or in any associated security equipment or the approved Ship security plan, without the sanction of the Authority.

Issue and Endorsement of Certificates

29. (1) An International Ship Security Certificate shall be issued after the initial or renewal verification is carried out under Regulation 28(1).

(2) The International Ship Security Certificate shall be issued or endorsed by the Authority or by an authorized Recognized Security Organization acting on behalf of the Government of Sri Lanka.

(3) The Authority may request another Contracting Government to carry out verification and, if satisfied that Regulation 28(1) are complied with, and 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 this Regulation:

(a) a copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the Authority;

(b) the certificate issued shall contain a statement to the effect that it has been issued at the request of the Authority; and

c) the certificate issued under this regulation shall have the same force and receive the same recognition as the certificate issued under sub-regulation (1).

(4) The International Ship Security Certificate shall be in the form prescribed in Schedule 4.

Duration and Validity of Certificate

30. (1) The International Ship Security Certificate shall be issued for a period determined by the Authority or the authorized Recognized Security Organization which shall not exceed 5 years from the date of its issue.

(2) When the renewal verification is completed:

(a) within 3 months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the duration and validity of certificate verification to a date not exceeding 5 years from the date of expiry of the existing certificate;

(b) after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the verification to a date not exceeding 5 years from the date of expiry of the existing certificate;

(c) more than 3 months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the verification to a date not exceeding 5 years from the date of completion of the renewal verification.

(3) If the Authority or the Recognized Security Organization issues a certificate for a period of less than 5 years, the Authority or the Recognized Security Organization may extend the validity of the certificate to the maximum 5 years period specified in sub regulation (1).

(4) If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry of the existing certificate, the Authority or the

Recognized Security Organization acting on behalf of the Authority may endorse the existing certificate which shall be accepted as valid for a further period not exceeding 5 months from the date of expiry of the certificate.

(5) If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Authority or the Recognized Security Organization may, if satisfied that it is reasonable to do so, extend the period of validity of the certificate for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified.

(6) No certificate shall be extended under sub-regulation (5) for a period longer than 3 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.

(7) When the renewal verification is completed in respect if a ship whose period of validity of certificate was extended under this regulation, the new certificate shall be valid for a period, not exceeding 5 years, from the date of expiry of the existing certificate before the extension was granted.

(8) A certificate issued to a ship engaged on short voyages which has not been extended under the provisions of this Regulation may be extended by the Authority or the Recognized Security Organization in consultation with the Authority for a maximum period of one month from the date of expiry of the certificate.

(9) When the renewal verification is completed in respect of a ship referred to in sub-regulation (8), the new certificate shall be valid for a period, not exceeding 5 years, from the date of expiry of the existing certificate before the extension was granted.

(10) If an intermediate verification is completed before the period specified in Regulation 28(1) (c), then:

> (a) the expiry date shown in the certificate shall be amended by endorsement to a date which shall not be more than 3 years later than the date on which the intermediate verification was completed;

(b) 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 Regulation 28(1) are not exceeded.

(11) A certificate issued under Regulation 28 shall cease to be valid in any of the following cases:

(a) if the relevant verifications are not completed within the period specified under Regulation 28(1);

(b) if the certificate is not endorsed in accordance with Regulation 28(1)(c) and sub-regulation(10)(a), if applicable;

(c) when a company assumes the responsibility for the operation of a ship not previously operated by that Company; and

(d) upon transfer of the ship to the flag of another State.

(12) In the case of:

(a) a transfer of a Sri Lankan ship to the flag of another Contracting Government, the Authority shall as soon as possible transmit to the Administration of such Contracting Government, copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports; or

(b) 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 regulation 28.

Interim Certification

31. (1) The Authority may cause an Interim International Ship Security Certificate, in the form prescribed in Schedule 5, to be issued in accordance with this Regulation, when:

(a) a Sri Lankan ship without a certificate, on delivery or prior to its entry or re-entry into service;

(b) transfer of a Sri Lankan ship to the flag of another Contracting Government;

(c) transfer of a Sri Lankan ship to the flag of a non-Contracting Government; or

(d) when a Company assumes the responsibility for the operation of a ship not previously operated by that Company, until the certificate referred to in Regulation 29 (1) is issued.

(2) An Interim International Ship Security Certificate shall only be issued when the Authority or the Recognized Security Organization on behalf of the Authority, has verified that:

(a) the ship security assessment required by these Regulations has been completed;

(b) a copy of the Ship security plan meeting the requirements of Chapter XI-2 of the Convention and these Regulations is provided on board, has been submitted for review and approval, and is being implemented on the ship;

(c) the ship is provided with a ship security alert system meeting the requirements of Chapter XI- 2/6 of the Convention, if required;

(d) the Company Security Officer:

(i) has ensured -

(A) the review of the Ship security plan for compliance with this Regulation;

(B) that the plan has been submitted for approval;

(C) that the plan is being implemented on the ship; and

(ii) 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 Regulation 28 (1) (a) within 6 months;

(e) arrangements have been made for carrying out the required verifications under Regulation 28 (1) (a);

(f) 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 Regulation, and with the relevant provisions of the Ship security plan placed on board, and have provided such information in the English language and the working language of the ship's personnel or languages understood by them; and

(g) the Ship Security Officer meets the requirements of these Regulations.

(3) An Interim International Ship Security Certificate shall be valid for 6 months, or until the certificate required by Regulation 29 is issued, whichever comes first, and shall not be extended.

(4) The Authority shall not cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the opinion of the Authority or the Recognized Security Organization in consultation with the Authority, the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with Chapter XI-2 of the Convention and these Regulations beyond the period of the initial interim certificate as specified in sub-regulation (3).

(5) The Authority may prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the requirements of sub-regulation (2) (d), (e) and of (f) have been met.

Sinhala Text to Prevail in case of Inconsistency

32. In the event of any inconsistency between the Sinhala and Tamil texts of these Regulations, the Sinhala text shall prevail.

SCHEDULE 1

[Regulation 3(1)]

FORM OF 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 (list the activities with relevant details)-
……..…
……..……
……..……
……..……
……..……
……..

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 Ship Security Officer or Port facility Security Officer under these columns indicates that the activity will be done, in accordance with relevant approved plan, by;	
Activity	*Port facility*	*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 facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handing of Cargo		
Delivery of Ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both port facility and the ship during the specified activities meet the provisions of chapter XI-2 and 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 …….. Day of …….20……

Signed for and on behalf of

Port facility:	Ship:
(Signature of the Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*

Name and title of person who signed

Name:	Name:
Title:	Title:

*(*This form of declaration of security if for use between a ship and a port facility. If the declaration of security is to cover two ships, this model should be appropriately modified)*

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:

[83] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Appendix to Part B, Appendix 1.

SCHEDULE 2

[Regulation 5(1)]

FORM OF CERTIFICATE OF COMPLIANCE

CERTIFICATE OF COMPLIANCE

Certificate No ……

Issued under the provisions of Part B of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS

AND OF PORT FACILITIES (ISPS CODE)

GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Sri Lankan Merchant Shipping Secretariat

Name of the 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 <specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):

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 issuing authority, as appropriate, must be affixed)

[84] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Appendix to Part B, Appendix 2.

SCHEDULE 3

[Regulation 5(2)]

FEES AND CHARGES FOR AUDIT OF PORT FACILITIES AND SHIPS

Item	Prescribed Fees	Rate Rs. (VAT Exclusive)
A	Initial audit of port facilities	**[500,000.00]**
B	Annual verification audit of port facilities	**[200,000.00]**
C	Initial audit for ships	**[50,000.00]**
D	Annual verification audit for ships	**[20,000.00]**
E	Application, assessing and issuance of certificates for port facilities and ships	**[20,000.00]**

Cost of transportation, meals and accommodations for Auditors shall be borne by the operators of Port facilities and ship owners and operators.

[85] In consonance with the fines prescribed in Fiji, Maritime (ISPS Code) Regulations 2014.

SCHEDULE 4

[Regulation 29(4)]

FORM OF INTERNATIONAL SHIP SECURITY CERTIFICATE

INTERNATIONAL SHIP SECURITY CERTIFICATE

Certificate No……

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 THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

by Sri Lankan Merchant Shipping Secretariat

Name of Ship:……

Distinctive number or 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 any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of the Chapter XI-2 of the SOLAS 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 19.1.1 of Part A of the ISPS Code

Issued at:…….. Date of issue:……..

(Place of issue of the certificate)

*(*Signature of the duly authorized 0fficial issuing the Certificate)*

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1 of Part A of the ISPS Code, the ship was found to comply with the relevant provisions of the Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

Intermediate Verification
Signed: ……..

*(*Signature of authorized 0fficial)*

Place:……..
Date:……...

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR INTERMEDIATE VERIFICATION**

Additional Verification
Signed:……...
*(*Signature of authorized 0fficial)*

Place:……..
Date:……...

Additional Verification
Signed:……...
*(*Signature of authorized 0fficial)*

Place:…….
Date:……...

Additional Verification
Signed:……...
*(*Signature of authorized 0fficial)*

Place:……..
Date:……...

*(** This part of the certificate shall be adapted by the Designated Authority to indicate whether it has established additional verifications as provided for in section 19.1.1.4 of Part A of the ISPS Code)*
*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF THE ISPS CODE

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

Signed:……
*(*Signature of authorized 0fficial)*

Place:……...
Date:……

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES

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

Signed:……
*(*Signature of authorized 0fficial)*

Place:……...
Date:……

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/19.3.4 OF THE ISPS CODE APPLIES

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

Signed:……...
*(*Signature of authorized 0fficial)*

Place:…….
Date:……..

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF THE ISPS CODE APPLIES OR FOR PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS CODE APPLIES

The Certificate shall, in accordance with section 19.3.5/19.3.6 (delete where appropriate) of Part of A of the ISPS Code, be accepted as valid until……

Signed:……
*(*Signature of authorized 0fficial)*

Place:……...
Date:……

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

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

Signed:…….
*(*Signature of authorized 0fficial)*

Place:……...
Date:……

*(** In case of completion of this part of the certificate, the expiry date shown on the front of the Certificate shall also be amended accordingly)*

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

[86] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Appendix to Part A, Appendix 1.

SCHEDULE 5

[Regulation 31(1)]

FORM OF INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

Certificate No.....

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 THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA by
Merchant Shipping Secretariat of Sri Lanka

Name of Ship: .....

Distinctive number or letters:.....

Port of registry: .....

Type of Ship: .....

Gross tonnage:.....

IMO Number:.....

Is this a subsequent, consecutive interim certificate? Yes/No
If Yes, date of issue of initial interim certificate:.....

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

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

This Certificate is valid until.....

Issued at: .....
(Place of issue of the certificate)

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

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

[87] IMO 'International Ship and Port Facility Security Code and SOLAS Amendments to 2002' (2003 edn) Appendix to Part A, Appendix 2.