UNDERSTANDING THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE:

AN EXAMINATION OF THE IMPLEMENTATION AND EFFECTIVENESS OF THE ISPS CODE

SHANTAL RAMSAROOP

201292909

Mini Dissertation submitted in 2016 to the School of Law in fulfilment of the requirements of the degree of Master of Laws in Maritime Law

College Of Law and Management Studies

School Of Law

Unit of Maritime Law and Maritime Studies

Supervisor: Mrs Deepa Lamb

I. DECLARATION OF ORIGINALITY

I, Shantal Ramsaroop, declare that:

I. The research reported in this thesis, except where otherwise indicated, is my original work.

II. This thesis has not been submitted for any degree or examination at any other university.

III. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

IV. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then: a) their words have been re-written but the general information attributed to them has been referenced; b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

V. Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

VI. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Candidate: Shantal Ramsaroop

Signature: …….

Date: …….

II. DEDICATION

"**Education is the most powerful weapon which you can use to change the world."**

Nelson Mandela

III. ACKNOWLEDGEMENT

I would like to express my gratitude towards many people who played a significant role during my study period in completing my dissertation, LLM:

- Firstly, Shri Sathya Sai Baba, my God, for his grace and blessings.
- Secondly, my sincere appreciation to my distinguished supervisor, Ms Deepa Lamb who guided me in writing the dissertation and provided me with invaluable advice and comments.
- Thirdly, my parents, Mr and Mrs Naicker who were of great support throughout my studies, I have a debt of gratitude for especially the baby-sitting of Saiesh while I studied.
- Finally I wish to express my deepest gratitude to my loving and encouraging husband Ravi.

I understand that the dissertation is not the final stage of my academic journey but in essence a new bright beginning. I will not forget all the experiences as well as the sense of accomplishment in the process of preparing for examinations, making presentations and writing this dissertation. I do believe every single moment of this process forms an invaluable baseline of my life in academia.

IV. ABSTRACT

It all started with a bang! Maritime security drastically evolved due to the tragic events of 11 September 2001(9/11), when a series of coordinated terrorist attacks were made on the United States of America. This unprecedented and catastrophic incident of terrorism shocked the world but more importantly drew the attention of the international maritime security authorities to the vulnerabilities of the seaports to acts of terrorism and other criminal threats.

The most significant international agreement relating to maritime safety and security is the 1974 International Convention for the Safety of Life at Sea (SOLAS), and this agreement was amended in 2002 in London, to include a new provision, that is the International Ship and Port Facility (ISPS) Code. The ISPS Code is in essence a framework of maritime security measures designed to enhance the security of ships and port facilities.

This dissertation is a study of the ISPS Code, an analysis of the regulatory provisions of the ISPS Code, its implementation and impact. The ISPS Code was implemented on 01 July 2004 and currently applies to 162 States that are contracting governments to SOLAS. This study has four chapters, chapter one sets out the background to the development of maritime security and it includes a regional perspective on maritime security as well as a status update on the main commercial ports in South Africa. Thereafter, chapter two is dedicated to providing the reader with an understanding of the provisions of the ISPS Code, describing its purpose, objectives and key elements.

Chapter three focuses on maritime security and terrorism. It provides the reader with summaries of maritime incidents that occurred prior to the implementation of the ISPS Code as well as incidents that took place after its implementation in order to assess its success in achieving its objectives of enhancing international maritime security. Finally chapter four provides a detailed analysis of the implementation and impact of the ISPS Code in South Africa as well as it implementation in other signatory countries of SOLAS such as Singapore, Iran and the United Kingdom. This chapter then concludes with recommendations made to the International Maritime Organisation to enable it to improve on its mandate of maritime security.

CONTENTS

CHAPTER 1: BACKGROUND TO THE DEVELOPMENT OF MARITIME SECURITY IN TERMS OF THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

1.1 *Introduction*

This chapter provides the background knowledge on the development of the ISPS Code from an international, a regional and thereafter a South African perspective. There is a brief layout of South African legislation relevant to maritime security as well as the current status of its main commercial ports.

1.2 *International Perspective on Maritime Security*

The first modern instance of vessel hijacking that attracted international attention was the seizure of the Portuguese passenger liner Santa Maria in January 1961.[1] Then in 1985, the hijacking of the cruise ship Achille Lauro[2] resulted in the development of the Convention on the Suppression of Unlawful Acts against the Safety of Maritime Navigation (the SUA Convention).

Maritime security drastically evolved due to the catastrophic events of 11 September 2001(9/11), when a sequence of synchronised terrorist attacks were made in the United States of America, specifically on the World Trade Centre and the Pentagon by the extremist Islamic terrorist group al-Qaeda. This unprecedented and catastrophic incident of terrorism shocked the world, but importantly drew the attention of the international maritime security authorities to the vulnerabilities of seaports to acts of terrorism and other criminal threats.

[1] L Joubert 'The extent of maritime terrorism and piracy: a comparative analysis' (2013) *Journal of Military Studies* Vol 41, No 1 pp111-137 at 118. Colonel Galvao and a group of 24 Portuguese insurgents hijacked the Santa Maria. The Colonel and his insurgents planned on overthrowing the government of Portugal (the Salazar regime) with the intention to sail the vessel to Angola. An officer was killed and a crew member was injured. There was difficulty in handling this case as it could not be defined as piracy since it was of a political nature.

[2] On 7 October 1985, the Italian MS Achille Lauro liner was hijacked while sailing from Alexandria to Ashdod, Israel by four men from the Palestine Liberation Front (PLF). This incident was recorded in history as one of the first terrorist acts. JPB Coelho *African Approaches to Maritime Security: Southern Africa* (2013) and D C Turack 'Maritime Terrorism and International Law' (1992) 41 (2) *The International and Comparative Law Quarterly* 490 FES Peace and Security Series 12: 5. The SUA Convention was intended to ensure that responsible authorities extradites or prosecutes persons responsible for committing terrorist acts at sea.

The United Nations General Assembly convened an emergency session on 12 September 2001 aimed at condemning the 9/11 attacks on the United States of America and adopting resolutions to enhance global maritime security.[3] A delegation from South Africa was present during this session.[4] Thereafter, there were various platforms in which engagements occurred in relation to the discussions of methods to enhance maritime security. It was decided that the best method for the enhancement of worldwide maritime security was to develop it at an international level.[5]

The International Convention for the Safety of Life at Sea (1974) is one of the most significant international maritime agreements relating to security and safety. This Convention was first adapted in 1914 in reaction to the Titanic disaster then a second adaptation in 1929, third adaptation in 1948, fourth adaptation in 1960 and finally the fifth and current adaptation in 1974. SOLAS has been amended on numerous occasions in order to meet the maritime industry needs and is currently named SOLAS 1974, as amended.[6] After the tragic incident of the 9/11 attacks, this significant Convention was again amended to include the International and Port Facility Security (ISPS) Code by the International Maritime Organisation (IMO), which took the lead in formulating numerous security related recommendations and Conventions by engaging states in discussions to develop international conventions designed to enhance international maritime security.[7]

These new provisions in the SOLAS, 1974 as amended and the inclusion of the International Ship and Port Facility Security Code (ISPS) were adopted during a Diplomatic Conference on Maritime Security in December 2002 in London.[8] This new security regime for the protection of both merchant ships and seaports was implemented on 01 July 2004[9] and was

[3]D L Bryant 'Historical and Legal Aspects of Maritime Security' *17 U.S.F Maritime Law Journal* (1) 2004-2005 at 10.

[4]General Assembly Press Release GA/9903, United Nations, Opening its Fifty-Sixth Session, 'General Assembly Condemns Heinous Acts of Terrorism Perpetuated in Host City and Washington' 2001 available at http://www.un.org/News/Press/docs/2001/ga9903.doc.htm (accessed on 19 May 2015).

[5]T J Schoenbaum and J C Langston 'An All Hands Evolution: Port Security in the Wake of September 11th' 2002-2003 77 *Tulane Law Review at* 1345.

[6] History and Background of the SOLAS Convention 1974 is available at: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx (accessed on 23 January 2015).

[7]R Balkin 'The International Maritime Organisation and Maritime Security' 2006 Tulane *Maritime Law Journal 30* at 3.

[8] 'Conference of Contracting Governments to the International Convention for the Safety of Life at Sea 1974' (2002) available at www.un.org.

[9]The IMO website have numerous documents on the topic of Maritime Security 'Maritime Security and Piracy' available at http://www.imo.org/ourwork/security/Pages/MaritimeSecurity.aspx (accessed on 23 April 2015).

effective in 147 States. Currently these new security measures apply to 162 Member States of SOLAS that are contracted to comply with the requirements set out in the ISPS Code.[10] At the Intersessional Working Group Conference on Maritime Security during 9-13 September 2002, the ISPS Code was described as an establishment of a worldwide framework that encompasses the co-operation between various key role-players such as contracting governments, government agencies, local administrations, shipping and port industries for the purposes of firstly, detecting security threats and secondly, ensuring that preventative measures are taken against security incidents that impact on ship and port facilities.[11]

The ISPS Code is in essence a framework of maritime security measures designed to improve port facilities and ships security.[12] This Code contains detailed and comprehensive security-related requirements for governments, shipping companies and port authorities. It is further divided into two parts, namely,

- Part A: Comprises of certain obligatory provisions, reference of which is also made in chapter XI-2 of SOLAS, 1974 as amended. This part creates the new global structure of measures to improve maritime security. This is achieved by ships and port facilities working jointly for the purpose of detecting and thereafter deterring security threats in the maritime transport sector.[13]

- Part B: This section fleshes out the contents of Part A and is non-mandatory but recommendatory.[14] However, some countries are considering making Part B mandatory whilst other countries like the USA have already made Part B mandatory.[15] Korea[16], the European Parliament and the Council of the European Union[17] have made some provisions of Part B mandatory in their national legislations.

[10] Ibid.
[11] Press Release IMO, 'Maritime Security Measures Take Shape at IMO' (2002) available at http://www.imo.org/blast/mainframe.asp?topic_id=583&doc_id=2435 (accessed on 20 May 2015).
[12] Maritime Port Authority of Singapore 'Port Security: ISPS Code' available at www.mpa.gov.sg (accessed on 06 February 2015).
[13] Part A of the ISPS Code s1, 1.1 – Guidance regarding the provisions of Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended and Part A of this Code.
[14]Transnet National Port Authority 'A World Class Port Security Service' (2007) available: http://www.transnetnationalportsauthority.net/DoingBusinesswithUs/Pages/Security.aspx (accessed on 17 February 2015).
[15]Most provisions of Part B of the ISPS Code are enforced in the United States Maritime Transport Security Act of 2002 Q van der Merwe, 'ISPS Code- Maritime Security' (2003) available: http://ports.co.za/legalnews/article_2003_08_15_1144.html (accessed on 18 February 2015).

1.3 *Regional Perspective on Maritime Security*

The Southern African Development Community (SADC) is utilised as a driving force for economic integration in Southern Africa since its existence in the year 1980. The SADC Treaty, specifically Article 5 provides objectives to realise integrated economic security within the region, of most relevance is the objective to promote and defend peace and security.[18]

In Angola, Luanda, during 2011, the Heads of State signed the SADC Maritime Security Strategy. South Africa together with Tanzania and Mozambique have been in collaboration on a number of maritime security related projects including maritime security and anti-piracy operations in the Indian Ocean, which is of vital importance as it is the earth's third-largest ocean and transports half of the world's trade in oil.[19]

The SADC Maritime Security Strategy is progressing well as a number of countries at the 20th Standing Maritime Committee meeting in Lusaka, Zambia during 4-5 April 2014 have signed cooperation agreements that include:

- The establishment of Maritime Domain Awareness Centres (MDACs) in Mozambique and Tanzania which are to be connected with those in Cape Town and Durban.
- Co-operational framework signed between Botswana, Lesotho, Zambia, Zimbabwe and Malawi.
- A memorandum of understanding between South Africa, Angola and Namibia on maritime cooperation aimed at addressing maritime security on the West Coast.[20]

---

[16] J Jibkwon 'Progress and Challenges: Ten years after the ISPS Code' (2013) World Maritime University, Sweden 20 available at http://dlib.wmu.se/jspui/bitstream/123456789/836/1/77473.pdf (accessed on 27 May 2015).

[17] C Pohlit 'New Developments in Maritime Security and the Impact on International Shipping' Dissertation submitted at University of Cape Town 26, available at http://uctscholar.uct.ac.za/PDF/1373_Pohlit.pdf (accessed on 28 April 2015). Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on Enhancing Ship and Port Facility Security.

[18] KJ Watson 'Promoting the Creation of an integrated Maritime Security Capability on the Southern African Coast' (2011) Conference.

[19] L Louw-Vaudran 'What does ensuring SADC's maritime security mean for South Africa?' (2014) available at http://www.issafrica.org/iss-today/what-does-ensuring-sadcs-maritime-security-mean-for-south-africa (accessed on 03 May 2015).

[20] Ibid.

1.4 *South African Maritime Legislative Framework*

In South Africa, the following legislation plays a significant role in ensuring maritime security:

- The Constitution of South Africa Act 108 of 1996, which is the supreme law of South Africa and provides the legal foundation for the existence of the Republic and which all laws in the Republic have to be in line with.

- The National Ports Act 12 of 2005, which provides for the establishment of the National Ports Authority and the Ports Regulator as well as to provide for the administration of certain ports by the National Ports Authority. In addition, the essential objective of this Act is to promote the development of an effective and productive port industry in South Africa that is capable of contributing to the economic growth and development of our country.[21]

- The Merchant Shipping (Maritime Security) Regulations, 2004 derived from the Merchant Shipping Act of 1951. The objectives of the Regulations include the implementation of the ISPS Code in order for South Africa to comply with its international obligations under Chapter XI-2 of the Safety Convention.

1.5 *South African Maritime Interest*

Due to South Africa's internal race policies, the United Nations actively promoted the exclusion of South Africa from international conventions and encouraged boycotts against the country.

After a long struggle for freedom, South Africa finally unlocked itself internationally after it held its first democratic elections in April 1994, only then was South Africa exposed to global trends.[22] Its maritime zones, spreading out to the edge of the continental shelf, including the exclusive economic zone, encompass an area of over 1 million square

[21] National Ports Act 12 of 2005, Section 2 Objectives at 10.
[22] A Minnaar 'Border Control and Regionalism, The Case of South Africa' (2001) 10 (2) *African Security Review.*

kilometres.[23] This massive ocean domain is potentially rich in natural resources, and environmentally of significant global importance.[24]

International trade is essential for many African economies and over 90% of Africa's exports and imports take place at sea.[25] The ports therefore play an extremely important role in the economics of the country. The international community looks to South Africa to be a leader in cultivating change and progress, not just in Southern Africa, but in the entire continent as well.

South Africa currently identifies itself as an essential component of the African continent and as a result comprehends its national interest as being fundamentally connected to Africa's maritime security. In order to maintain international standards, South Africa, being a signatory to the IMO, has ratified the ISPS Code. The following are some reasons for ratifying the ISPS Code:

- Vessels visiting ports that are non-compliant with the ISPS Code could be viewed as a security risk and could be turned away at ports that are compliant to the Code.[26]
- A ship may be declared unsafe for visiting a port that is non-compliant with the ISPS Code, which would result in it losing its insurance cover and would expose it to third party claims.[27]
- Furthermore, failure of a port to comply with the ISPS Code may constitute prima facie proof of negligence, which would result in a charterer having recourse to sue the port.[28]
- Non-compliance with the ISPS Code may result in ship operators avoiding that port in an effort to avoid experiencing delays.

[23] M Siko 'South Africa's Maritime Interests and Responsibilities' (1996) at 5 *African Security Review.*
[24]C Forrest 'The Balancing of Maritime Interests in the Southern African Oceans in Light of the New International Maritime Security Regime' (2008) 41 (1) *The Comparative and International Law Journal of Southern Africa* at 6.
[25] 'Africa's ports vital for world trade' (2015) available at www.itonline.co.za (accessed on 13 April 2015).
[26]Q van der Merwe 'ISPS Code- Maritime Security' (2003) available: http://ports.co.za/legalnews/article_2003_08_15_1144.html (accessed on 18 February 2015).
[27] N Karigithu 'Port Security – The ISPS Code' (2008) available at www.pmaesa.org/media/.../Kenya_Maritime_Authority_Djibouti_2008 at Slide 23, (accessed on 04 April 2015).
[28]Ibid.

The ISPS Code has been implemented in South Africa through the Merchant Shipping (Maritime Security) Regulations, 2004, which is provided for in the Merchant Shipping Act 57 of 1951.[29] The National Department of Transport is the selected custodian for implementing the ISPS Code as per the National Ports Act 12 of 2005.[30]

The Department of Transport as custodian, developed methods to encourage maritime transport and as such, allocated the operational aspects of maritime transport responsibilities to various government agencies such as the South African Maritime Safety Authority (SAMSA), Transnet National Ports Authority (TNPA), Transnet Port Terminal (TPT) and the South African Ports Regulator.[31]

1.6 *Status of Commercial Ports in SA*

Transnet National Ports Authority is in terms of section 3(1) of the National Ports Act, 2005 (Act No. 12 of 2005), a port authority which owns, manages, controls and administers all ports within the Republic to ensure their efficient and economic functioning. South Africa has eight commercial ports that are all managed by TNPA. Maritime security plans are in place at these ports and implemented by the relevant port facilities and service providers.[32] The TNPA succeeded in certifying South Africa's eight major ports as compliant with the ISPS Code at a cost of over R200 million.[33]

South Africa's eight main commercial ports are:

- Richards Bay
- Durban
- East London
- Port Elizabeth
- Mossel Bay
- Cape Town
- Saldanha Bay
- Ngqura

[29] Forrest op cit n 24 at 11.
[30] Transnet National Port Authority op cit n 14.
[31] Draft South African Maritime Transport Policy (2008).
[32] Transnet National Ports Authority Presentation op cit n 14 at slide 6.
[33] Forrest op cit n 24.

South Africa acknowledges that neglecting maritime security can result in a loss of economic prospects as well as grave economic threats,[34] so it is making a concerted effort in ensuring that it complies with international standards, as well as ensuring that all role-players have a common understanding on the implementation of such regulations. This is evident in a number of documents/notices that are in place to ensure compliance as well as an understanding of the ISPS Code and other relevant International Maritime Security Codes and Regulations:

- TNPA has issued an ISPS Vessel Clearance Procedure, Policy Number: SMP 3/2010 with the objective of ensuring that all the ports falling within the jurisdiction of the TNPA adhere to the same procedures when dealing with maritime security regulated vessels intending to call in any of these ports. (See Annexure 1).

- SAMSA Marine Notice 12 of 2008, the Merchant Shipping (Maritime Security) Regulations, 2004 provides guidance to the maritime industry on the application of the Merchant Shipping (Maritime Security) Regulations, 2004 and the ISPS Code (See Annexure 2). Specific guidance is provided on various maritime security related matters including:
    - Certification of South African Ships
    - Security Level in South African Territorial Waters
    - Port Security

- SAMSA Marine Notice No. 20 of 2014; Unlawful Interference with Maritime Transport – Stowaways, SOLAS Chapter XI-2 Maritime Security (See Annexure 3). This notice informs all ship owners, masters and agents on maritime security regulations related to the following:
    - SOLAS Chapter XI-2: Special Measures to Enhance Maritime Security.
    - ISPS Code, Part B, item 8: Ship Security Assessment
    - ISPS Code, Part B, item 9: Ship Security Plan

- SAMSA Marine Notice 5 of 2015, Procedures to be followed for Bulk Cargo Shipment which are not listed in the International Maritime Solid Bulk Cargoes Code.

[34]JPB Coelho 'African Approaches to Maritime Security: Southern Africa' (2013) 12 FES *Peace and Security* at 5.

This notice clears the confusion within the shipping industry on the statutory procedures of compliance for the shipment of solid bulk cargoes which are not listed in the International Maritime Solid Bulk Cargoes Code (Code published by the IMO) (See Annexure 4).

1.7 *Conclusion*

The development of the ISPS Code has resulted in an international consensus on the methodology of securing the maritime environment; this methodology is that of compliance with the regulation of the ISPS Code. In addition, market forces and economic factors will also play a role in ensuring compliance with the ISPS Code.[35] With the increasing number of contracting states to the SOLAS, it is inevitable that these new security measures, as part of the ISPS Code will soon be embodied in most of the maritime communities' national legislations, as all those involved in the maritime industry strive to protect trade at sea and be recognised as complying with international conventions.

South Africa is at an advanced stage of implementation and compliance with the ISPS Code as it has already created its domestic legislation. The Merchant Shipping Regulations 2004 embodies the critical provisions of the ISPS Code and more importantly, all of South Africa's commercial ports are compliant to the provisions of the ISPS Code. Furthermore, South Africa's participation in international forums, reaffirms its intention of ensuring that its levels of maritime security compliance standards are of an international level and this is maintained. South Africa actively participates in various forums focusing on the enhancement of maritime security, such as the International Labour Organisation (ILO), Abuja Memorandum of Understanding on Port State Control, Southern African Transport Co-ordinating Committee (SATCC), International Maritime Organization (IMO) and the Indian Ocean Memorandum of Understanding (IOMOU) on Port State Control.[36]

[35] International Maritime Organization IMO: 'ISPS Code and Maritime Security' available at www.imo.org/Newsroom/mainframe.asp?topic_id=897 (accessed on 26 April 2015).
[36] Draft South African Maritime Transport Policy (2008) Section 1 at 7.

CHAPTER 2: UNDERSTANDING THE PROVISIONS OF THE ISPS CODE

2.1 *Introduction*

Maritime security is an international responsibility and as such, there exist an international legal framework wherein one of the most important regulations is the SOLAS Chapter XI-2 amendments that contain the ISPS Code.

The ISPS Code is divided into two parts, Part A is mandatory whilst Part B is recommendatory. This chapter will provide an understanding of each regulation in terms of the ISPS Code, thereafter due to the importance of Part A being mandatory, further commentaries will be provided for a deeper understanding and meaning of the applicable provisions and in certain instances, the practical ways in which states employ these measures.

It is important to note that the ISPS Code requires cooperation between Governments, government agencies, local administrations, shipping and port industries.[37] A number of the provisions of the ISPS Code are in fact previous recommendations made by IMO following the hijacking of the Achille Lauro in 1986. Some of these provisions include an obligation on member states to ensure that there are security plans and appointed security officers for their ship and port facilities. The actual process in the ISPS Code of ensuring security of the port facilities and ship is essentially a risk management activity, which is conducted by assessing the risks in order to determine the appropriate security measures required.[38]

2.2 *Purpose of the ISPS Code*

Due to the acts of terrorism directed at the United States of America, the international body of maritime security, the International Maritime Organisation (IMO), developed security measures to protect vessels in the world fleet and global port facilities from such criminal acts. The security measures have been incorporated in the amendments to the Safety of Life at Sea Convention, 1974 (SOLAS Convention). A new international framework of measures to enhance maritime security was created by the adoption of the ISPS Code. It is an

[37] H Hesse and N L Charalambous 'New Security Measures for the International Shipping Community' 2004 3 (2) *WMU Journal of Maritime Affairs* 123–138 at 123.

[38] International Maritime Organization 'Enhancing Maritime Security' available at http://www.imo.org/Newsroom/mainframe.asp?topic_id=582 (accessed on 25 April 2015).

instrument through which ships and port facilities can co-operate with each other to detect and deter acts which threaten security in the maritime transport sector.[39]

2.3 *Objectives of the ISPS Code*

The objectives of the Code as stated in Part A:

1. "To establish an international framework involving co-operation between Contracting 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 facilities used in international trade;
2. To establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security;
3. To ensure the early and efficient collection and exchange of security-related information;
4. To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
5. To ensure confidence that adequate and proportionate maritime security measures are in place."[40]

Maritime security is a collective international responsibility and to ensure the success of a secure maritime environment, it is critical that security measures are consistent and standardised. The ISPS Code seeks to establish an international framework that can be utilised by the maritime community in relation to maritime security. It essentially provides for the detection and deterrence of security threats as well as a methodology of assessing security whilst establishing the roles and responsibilities of various parties. The ISPS Code enables the collection and the exchange of security information. It further ensures that adequate security measures are in place.[41]

[39] ISPS Code, Part B.
[40] ISPS Code, Part A op cit n 13 at 1.2 Objectives at 4.
[41] Lloyd's Register Marine 'ISPS Code' available at *http://www. lr.org/en/marine/compliance/standards-schemes-codes-and-directives/isps-code.aspx (*accessed on 25 May 2015).

2.4 *Security Levels*

The setting of the security level is the responsibility of the contracting government. The Code contains three security levels namely:

- Security Level 1: Normal: This is the typical operational level of ships and port facilities.[42] This level provides for minimum protective security measures to be sustained at all times. For a security level 1, the following activities should be carried out:
    - Access to the port facility should be controlled.
    - All port facility duties should be performed.
    - The supervision of the handling of ship stores and cargoes.
    - The restricted areas should be monitored in order to certify that only those that are authorised accordingly have access.
    - Security related communications should be readily available.
    - The port facility should be monitored.[43]

  In South Africa's territorial water and eight main commercial ports, Security Level 1 applies and any change of security level in the South African territorial water will be notified by Marine Notice, Navigational Warning and Notices to Mariners whilst any change in security level in South African ports will be declared by the Director General of Transport.[44]

- Security Level 2: Heightened: This level applies for the duration of the period of the heightened risk of a security incident.[45] This level provides for supplementary protective security measures to be sustained for a period of time.

- Security Level 3: Exceptional: This level is applicable for the duration of a probable or imminent risk of a security incident.[46] This level provides for additional particular protective security measures to be maintained for a period of time. Setting security level 3, according to the Code, should firstly only be applied when there is credible information

[42] ISPS Code, Part A op cit n 13 at 5.
[43] Specific guidelines are available at www.imo.org.za.
[44] South African Maritime Safety Authority, Marine Notice No.12 of 2008, the Merchant Shipping (Maritime Security) Regulations, 2004, Regulation 3.
[45] ISPS Code, Part A op cit n 13 at 6.
[46] Ibid.

that a security incident is probable or imminent and secondly only be set for the time period of the identified security threat/actual security incident.

The three levels defined above is as stated in the ISPS Code; however, a basic understanding of the levels would be Level 1 equals a low threat situation, whilst Level 2 amounts to a medium threat situation and Level 3 is a high threat situation. Since each ship and each port facility will have a different risk, it is the responsibility of the Contracting Government to determine and set up the security level. The security level set in fact creates a link between the ship and the port facility as it triggers the application of certain security measures for the ship and the port facility as per the ISPS Code regulations.

2.5 *Minimum Functional Security Requirements*

The ISPS Code comprises of numerous minimum functional security requirements for both ships and port facilities which can be viewed as part of Basic Risk Management activity.[47] Basic Risk Management principles can be divided in two elements, firstly to identify risks and secondly to quantify risks.[48] Therefore in the risk management process, an assessment of the risk needs to be conducted in order to determine suitable and correct security measures.[49] Training and drills are of vital importance in ensuring the application of these security requirements.[50]

Security Requirements in the ISPS Code:

- Ships require Ship Security Officers (SSO), Company Security Officers (CSO), Ship Security Plans (SSP) and certain onboard equipment.
- Port Facilities require Port Facility Security Officers (PFSO), Port Facility Security Plans (PFSP) and certain security equipment.
- Ships and Port Facilities require monitoring and controlling access, ensuring security communications and monitoring the activities of people and cargo.

---

[47] IMO 'IMO Adopts Comprehensive Maritime Security Measures' 2002 available at www.imo.org/blast/mainframe.asp?topic_id=583&doc_id=2689 (accessed on 07 May 2015). IMO stated that maritime security is a risk management system and that the ISPS Code is a support to SOLAS and each contracting government as a methodology to improve the response and the system performance concerning maritime security.

[48] P Hellberg 'Effects of the ISPS Code on Ship and Port Security – A Swedish Perspective' 2009 available at *http://dlib.wmu.se/jspui/bitstream/123456789/737/1/20052.pdf* (accessed on 25 May 2015) at 19.

[49] H Hesse and N L Charalambous op cit n 37 at 125.

[50] C Trelawny 'Maritime Security: Implementation of the ISPS Code' 2005 IMO 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference Dar es Salaam at 5.

2.6 *Key Elements of the ISPS Code*

The ISPS Code is 89 pages in length and is divided into two parts:

2.6.1 *Part A of the ISPS Code*

Part A comprises of obligatory requirements regarding the provisions of Chapter XI-2 of the SOLAS, 1974 as amended, that impose obligations on governments, shipping companies and port authorities. This part creates a new global structure of measures to improve maritime security through which port facilities and ships can work together to detect and deter acts which threaten security in the maritime transport sector.[51]

Part B of the ISPS Code is of vital importance and it is evident as throughout the provisions contained in Part A of the Code, reference is made to the specific guidance that is provided by Part B of the ISPS Code.

Part A is divided into 19 Regulations and includes 2 Appendixes, it covers the following:

Regulation 1: General
This section confirms that Part A is mandatory; it further provides the objectives of the code as well as the functional requirements needed in order to achieve its objectives.[52]

Regulation 2: Definitions
This is a standard definitions section providing an understanding on the various requirements of port and ship security plans and officers as well as the different security levels.[53]

Regulation 3: Application
Details are provided of the ships that would be subject to this Code as well as those ships that have been excluded. Contracting Governments are also provided with guidelines on application of the Code to port facilities. The ISPS Code is applicable to ships on international voyages which includes cargo ships of 500 GT and upwards, mobile offshore drilling units, passenger ships and the port facilities serving such ships. The ISPS Code is not

[51] ISPS Code, Part A op cit n 13 at 2.
[52] Ibid at Regulation 1 at 4.
[53] Ibid at Regulation 2 at 5.

applicable to warships, naval auxiliaries, other ships owned or operated by a Contracting Government and used only on Government non-commercial service.[54]

The application of the ISPS Code to certain vessels only, is a cause for concern, as it can be viewed as creating a loophole in the system. In the event of terrorists becoming aware of the fact that certain types of vessels are exempted from these enhanced security measures, they may use these vessels for their advantage. Some countries have taken cognisance of this loophole in the framework and acknowledged the possibility of the exempted vessels being utilised by terrorist and other criminal networks. So they have created their own set of enhanced maritime security measures, in Regulations specifically focusing on the vessels that fall outside the scope of the ISPS Code.

The IMO recognises the concern of vessels that fall outside the scope of the ISPS Code and have created guidelines on the security aspects to assist signatories to SOLAS in this regard. Its guideline comes in the form of a circular MSC.1/Circ.1283[55], with heading Non-mandatory guidelines on security aspects of the operation of vessels which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code. Other signatories to SOLAS like the United Kingdom are utilising this guideline by making it readily available for its users.

Regulation 4: Responsibilities of Contracting Governments (RSO)

Port facility security levels may vary from port to port therefore Contracting Governments are tasked with the responsibility of setting security levels and providing guidance for safeguarding against security incidents. Contracting Governments may further delegate certain responsibilities related to security to a Recognised Security Organisation (RSO). The responsibilities of the Contracting Governments include the communication of information, testing ship security plans, setting security levels, notification of security levels, and declaration of security. To determine the applicability of a Declaration of Security, the risk of the ship posing to people, property and the environment is assessed.[56]

There are factors that need to be taken in consideration when setting security levels, such as the potential consequences of the security incidents, whether the threat information is

[54] ISPS Code, Part A op cit n 13 at Regulation 3 at 6-7.
[55] IMO, MSC.1/Circ.1283 http://www.imo.org/blast/blastDataHelper.asp?data_id=24823&filename=1283.pdf (accessed on 06 October 2015).
[56] ISPS Code, Part A op cit n 13 at Regulation 4 at 7.

credible, specific/imminent, corroborated. [57] It is important to note that the duties of the Contracting Governments are crucial to the successful implementation of the ISPS Code.

In Singapore, the RSO is appointed by the Maritime Port Authority (MPA) to perform the following responsibilities:

- Issue International Ship Security Certificates to Singapore flagged ships on its behalf.
- Approve Ship Security Plan (SSP).
- Assist the Singapore MPA to complete security assessments, and formulate or endorse Port Facility Security Plan (PFSP) port facilities of Singapore. [58]

Regulation 5: Declaration of Security (DoS)

Contracting Governments are responsible for determining when a Declaration of Security is needed and this section provides for a method for Contracting Governments to do so, namely: evaluating the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment. This section also lists the circumstances under which the Declaration of Security can be requested. For instance the ship can request the DoS if there has been a security threat or security incident. The Declaration of Security shall further be completed by the Master or Ship Security Officer and the Port Facility Security Officer. The duration for which the Declaration shall be retained by ships shall be determined by the Administration. [59]

Regulation 6: Obligations of the Company

It is the obligation of the Company to ensure that certain details are provided for the compilation of the Ships Security Plan such as a clear statement highlighting the master's overriding authority and responsibility to make decisions regarding the ship's safety and security. Furthermore, the Company Security Officer, the Master and the Ship Security Officer shall be given the required support to fulfil their responsibilities.[60] Signatories to SOLAS, are developing methods of assisting the Company and Ship Security Officers in

[57]Additional guidance is provided in MSC/Circ. 1074 on Interim Guidelines for the authorization of RSOs available at www.imo.org.
[58] Maritime Port Authority of Singapore op cit n 12.
[59]ISPS Code, Part A op cit n 13 at Regulation 5 at 8.
[60]Ibid at Regulation 6 at 8-9.

compiling the Ship Security Plan, one of the methods utilised by the United Kingdom is making available model Ship Plans for various types of vessels.[61]

Regulation 7: Ship Security

Contracting Governments set security levels that a ship is required to act upon. Activities are listed for each security level[62] that are to be carried out in order to detect and take precautionary measures against security incidents. Security Level 1 provides for a list of seven activities that need to be carried out in order to identify and take preventative measures against security incidents. Whilst at Security Level 2 additional protective measures shall be implemented for each activity of Security Level 1. Security Level 3 requires further specific protective measures for each activity mentioned for Security Level 1. It is further noted that with each of the three security levels, guidance is provided in Part B of the Code which is recommended to be considered.[63]

In Malaysia, at Port Klang when a security level is increased, additional external support is required from the Federal Government which deploys various enforcement agencies to mitigate the risks.[64]

Regulation 8: Ship Security Assessment (SSA)

The Ship Security Assessment serves the purpose to develop and update the Ship Security Plan. The Company Security Officer is to ensure that the Ship Security Assessment is conducted by persons with suitable skills to assess the security of a ship. Note that the Recognised Security Organisation may also carry out the Ship Security Assessment. The Ship Security Assessment shall further be accordingly documented, reviewed and reserved by the Company. The SSA shall include an on-scene security survey as well as identification of a number of elements detailed in this section.[65]

---

[61] See templates for better understanding, published by the UK Department of Transport available at https://www.gov.uk/government/publications/model-ship-security-plan-templates (accessed on 06 October 2015).

[62] For an example for a security level 1: there should be supervision of the handling of cargo and ships stores, deck areas and areas surrounding the ship should be monitored, access to the ship should be controlled and restricted areas should be monitored in order to ensure that only authorised persons have access.

[63] ISPS Code, Part A op cit n 13 at Regulation 7 at 9-10.

[64] P Gunasekaran 'Port Security in a developing country pre and post 9/11 terrorist attacks: A Case Study on Port Klang in Malaysia' (2012), a Thesis submitted to the University of Greenwich, London at 170.

[65] ISPS Code, Part A op cit n 13 at Regulation 8 at 10-11.

The Ship Security Assessment further addressed the following fundamentals within or on board the ship: physical security, procedural policies, structural integrity, personnel protection systems, radio, telecommunication, computer systems and other areas.

Regulation 9: Ship Security Plan (SSP)

The Ship Security Plan is intended to safeguard various persons on board, as well as cargo and the vessel from the risks of security incidents. The purpose of a Ship Security Plan is to assist in preventing unlawful acts against the vessel, crew and passengers as well as to minimise damage to the port facilities and maritime environment.[66]

On board a vessel, there should be a Ship Security Plan that is approved by the Administration or a Recognised Security Organisation. The Ship Security Plan shall be protected from unauthorised access or disclosure and not subject to inspection under control and compliance measures. The Plan should contain a clear statement regarding the Masters superseding authority and responsibility to make pronouncements concerning the security of the ship. The plan should be written in the language or languages of the ship as well as make provisions for the three security levels.[67]

In the United Kingdom, the Maritime and Coastguard Agency (MCA) approves SSPs for UK-registered vessels whilst the UK Department for Transport (DfT) approves for passenger ships.[68]

Regulation 10: Records

Records should be retained for a period indicated by the Administration, be protected from unauthorised disclosure/access and be in a language or languages of the ship. Records of the following undertakings are addressed in the Ship Security Plan and should be maintained on board the vessel:

- Training, drills and exercises.
- Security threats, security incidents, breaches of security.
- Changes in security levels.
- Communications relating to the direct security of the ship.

[66] UK Maritime and Coastguard Agency 'Maritime Safety and Working Conditions' 2013 available at https://www.gov.uk/guidance/maritime-security (accessed on 07 October 2015) at 30.
[67] ISPS Code, Part A op cit n 13 at Regulation 9 at 11-13.
[68] UK Maritime and Coastguard Agency op cit n 66 at 30.

- Internal audits and reviews of security activities.
- Periodic review of the SSA and the SSP.
- Implementation of any amendments to the plan.
- Maintenance, calibration and testing of security equipment.[69]

Regulation 11: Company Security Officer (CSO)

The Company Security Officer is selected by the Company and based ashore with a threefold responsibility: firstly, to ensure that a Ship Security Assessment is duly conducted, secondly, that the Ship Security Plan is developed, approved, implemented and maintained. Thirdly, there should be liaison between the Ship Security Officer and the Port Facility Security Officer.[70]

In the United Kingdom, it is a government requirement that Company Security Officers undergo training that is approved in accordance to the Maritime Safety Committee (MSC)/Circular 1154.[71]

Regulation 12: Ship Security Officer

Each ship should have a designated Ship Security Officer whose duties include enhancing security awareness, making sure that all security incidents are reported and that suitable training has been provided to shipboard personnel.[72]This Ship Security Officer is also accountable to the Master for the security of the ship.

Regulation 13: Training, Drills and Exercises on Ship Security

Company Security Officer and the relevant shore-based personnel will receive training and be knowledgeable on security matters. Drills are to be carried out at appropriate intervals in order to ensure the effective application of the SSP. Company Security Officer shall further ensure effective coordination and implementation of the Ship Security Plan.[73] In some countries the maritime port authorities endorse a particular maritime training service provider to ensure that their personnel is adequately prepared with the requisite skills and knowledge. As such, the Maritime Port Authority of Singapore has training providers that have been

[69]ISPS Code, Part A op cit n 13 at Regulation 10 at 13.
[70]Ibid at Regulation 11 at 14.
[71] UK Maritime and Coastguard Agency op cit n 66 at 30.
[72]ISPS Code, Part A op cit n 13 at Regulation 12 at 15.
[73] ISPS Code, Part A op cit n 13 at Regulation 13 at 15-16.

endorsed to conduct training as per the IMO model requirements and the ISPS Code. This training is for the benefit of the Company Security Officers (CSOs), Ship Security Officers (SSOs) and Port Facility Security Officers (PFSOs) in furthering their mandate to enhance maritime security.[74]

The United Kingdom government has a list of approved training providers on their website and requires that the PFSO must complete a training course which has been approved by the Maritime and Transport Security (MTS) division, at the Department for Transport (DfT).[75]

Regulation 14: Port Facility Security

Contracting Governments are responsible to set the security levels. Security procedures and measures are to be instituted, so as to result in minimum interference with or delay to ship's personnel and visitors, passengers, ship, goods and services.[76]

Regulation 15: Port Facility Security Assessment (PFSA)

The Port Facility Security Assessment is the crucial part of the process of creating and updating the Port Facility Security Plan. The Assessment is to be conducted by the Contracting Government or allocated Recognised Security Organization with the appropriate skills.[77] The Port Facility Security Assessment is to be reviewed and updated periodically in order to accommodate for threat level changes as well as minor changes in the port facility.[78] It further identifies and evaluates the current existing threats, the current security measures that are in place and the important infrastructure and assets that require protection.

Regulation 16: Port Facility Security Plan (PFSP)

The PFSP is to be created and sustained based on the conclusion of the Port Facility Security Assessment for each port. The Port Facility Security Officer is responsible for the development as well as the revision of the PFSP. Provisions are made in the Port Facility

[74] Maritime Port Authority of Singapore op cit n 12.
[75] UK Department of Transport 'Security Training Requirements in UK Ports for Staff and Approved Training Providers' 2012 available at https://www.gov.uk/guidance/security-training-for-staff-working-in-ports (accessed on 06 October 2015).
[76] ISPS Code, Part A op cit n 13 at Regulation 14 at 16-17.
[77] Ibid at Regulation 15 at 17-18.
[78] IMO op cit n 43.

Security Plan for the three security levels. The Contracting Government is required to approve the PFSP. The PFSP is to be protected from unauthorised access or disclosure.[79]

The role of the PFSP is to make sure that the security measures developed are applied in order to safeguard the ships and port facility from risks of security incidents. In the United States of America, the Coast Guard, the agency that is responsible for vessel and facility security examines the high-risk foreign vessels and is tasked with the responsibility of ensuring that all visiting foreign vessels comply with the requirements of the ISPS Code.[80]

In Canada, the PFSP is named the Marine Facility Security Plan and is approved by Transport Canada Marine Safety and Security. The Marine Facility Security Officers is tasked with maintaining and updating the plans.[81]

Regulation 17: Port Facility Security Officer (PFSO)

The Port Facility Security Officer is tasked with the responsibility of ensuring the Port Facility Security Plan is developed, implemented, revised, maintained and liaised with the Company Security Officers and the Ship Security Officers. There should be a Port Facility Security Officer assigned to each port facility and be provided the necessary support to fulfil the duties. There is a list of responsibilities and duties that is allocated to the PFSO, this includes development, maintenance and implementation of the PFSP, inspection of the port facility, conducting security survey and enhancing security awareness of personnel.[82]

The PFSO play a significant role in maritime security, as illustration, in New Zealand, the PFSO are informed of international developments as well as issues as they develop, they also form part of the committee chaired by the Maritime Safety Authority, a platform for discussions and deliberations on maritime safety and security.[83]

---

[79] ISPS Code, Part A op cit n 13 at Regulation 16 at 18-19.

[80] American Association of Port Authority 'Five Years After 9/11 Attacks: U.S. Ports More Secure Than Ever; Progress must Continue' (2006) available at http://www.aapa-ports.org/Press/PRDetail.cfm?ItemNumber=1092 accessed on 07 October 2015.

[81] Port of Belledune, Canada 'Port Security' available at http://www.portofbelledune.ca/security.php accessed on 07 October 2015.

[82] ISPS Code, Part A op cit n 13 at Regulation 17 at 19-20.

[83] P William 'The Implementation of the ISPS Code in New Zealand and Regional Issues for Discussion' Presented to the government by the Deputy Director Safety and Response Services Maritime Safety Authority available at http://www.amsa.gov.au/aphomsa/archives/Meeting%207/Agenda%20Item%202%20Maritime%20Security/Implementation%20of %20IsPS%20Code(NZ).pdf (accessed on 15 September 2015) at 4.

Regulation 18: Training Drills and Exercises on Port Facility Security

The PFSO and port facility security personnel have to be trained and should have the requisite knowledge to conduct the required training drills and exercises at appropriate intervals. Drills ought to take place at least every three months. Exercises should be carried out annually. IMO currently provides guidance on training and certification for Port Facility Security Officers by means of the Maritime Security Circular 1/Circ.1188.[84]

Some States are proactive in ensuring standardised training is made available to their security personnel at various ports. This is illustrated in New Zealand, where the Maritime Authority, facilitates centralised training in order to ensure all are on the same level of understanding. In addition, it has developed port and ship planning guidelines that have been distributed to ship and port companies. [85]

Regulation 19: Verification and Certification for Ships

This section provides an understanding on verifications, issue and endorsement of certificate, duration and validity of certificate and interim certification.

- Initial Verification will comprise of a complete verification of its security system, associated security equipment and the approved SSP. There should be a satisfactory condition and fit for the service.

- Renewal Verification should not surpass five years. The security system and any related security equipment should be in compliance with the requirements. There should be a satisfactory condition and fit for service.

- Intermediate Verification consist of the inspection of system for security and any associated security equipment with a minimum of one intermediate verification, if one only, it will occur between the second and third anniversary date.

- Additional Verification as determined by the Administration.[86]

[84] IMO op cit n 43.
[85] ISPS Code, Part A op cit n 13 at Regulation 17 at 19-20.
[86] ISPS Code, Part A op cit n 13 at Regulation 19 at 21-25.

Appendix 1: Form of the International Ship Security Certificate – also containing additional endorsements if needed (See Annexure 5).

Appendix 2: Form of the Interim International Ship Security Certificate (See Annexure 6).

2.6.2 *Part B of the ISPS Code*

Part B is non-mandatory but recommendatory; it sets out guidelines on how the mandatory requirements of Part A might best be complied with. It essentially fleshes out the contents of Part A. This part is divided into 19 Regulations and 2 Appendixes.

Regulation 1: Introduction

The introduction includes the preamble of this Code and it provides guidance on the following:

- Responsibilities of Contracting Governments: There is a list of responsibilities that include the approval of the Ship Security Plans as well as the exercise of control and compliance measures. In addition, there is an exclusion list detailing duties or activities that cannot be delegated to a Recognised Security Organisation.[87]

- Setting the Security Level: There is an elaboration of the three security levels.

- The Company and the Ship: The Company must designate a Company Security Officer (CSO) and one Ship Security Officer per ship.

- The Port Facility: Port Facility Security Assessments is essentially a risk analysis that has to be completed by each Contracting Government. This section details the content of the assessment, it assists in the determination of which port facilities will be required to assign a Port Facility Security Officer and develop a Port Facility Security Plan.[88]

- Information and Communication: Information is to be made accessible to allow for effective communication between the Contracting Governments as well as between

[87]ISPS Code, Part B op cit n 39 at Regulation 1 at 31-35.
[88]Ibid at Regulation 1 at 34.

Company/SSO and the Port Facility Security Officers. The Contracting Governments are also required to make available certain information to the IMO.[89]

Regulation 2: Definitions

There is no guidance provided regarding definitions in chapter XI-2 or part A of the ISPS Code however there is an elaboration of section, paragraph and Contracting Government.

Regulation 3: Application

This section provides guidance on ships and port facilities. The provisions of the ISPS Code do not apply to port facilities intended and utilised predominantly for military purposes.[90]

Regulation 4: Responsibilities of Contracting Governments

The following responsibilities of the Contracting Government are detailed:

- Security of Assessments and Plans
- Designated Authorities
- Recognized Security Organizations
- Setting security levels
- Contact points and information on Port Facility Security Plans
- Identification documents
- Fixed and floating platforms and mobile offshore drilling units on location
- Ships which are not required to comply with Part A of this Code
- Threats to ships and other incidents at sea
- Alternative security agreements
- Equivalent arrangements for port facilities
- Manning level
- Control and compliance measures
- Control of ships in port
- Ships intending to enter the port of another Contracting Government
- Additional provisions
- Non-party ships and ships below convention size[91]

[89] Ibid.
[90] Ibid at Regulation 3 at 35.
[91] ISPS Code, Part B op cit n 39 at Regulation 4 at 36-46.

Regulation 5: Declaration of Security (DoS)

The foremost purpose of the Declaration of Security is to ensure consensus between the relevant role-players regarding security measures. Completion of a DoS is required:

- In the event of the Contracting Government of the port facility or ship considering it to be required.
- The PFSA results may also indicate that a DoS is required whilst the reasons and circumstances for a DoS ought to be set out in the PFSP.
- A ship or its Administration may request a DoS.
- Port Facility Security Officer may initiate a DoS.[92]

Regulation 6: Obligations of the company

The Company is accountable for submitting information to the Master of the ship. The information is to comply with the requirements of the Company and include those responsible for appointing shipboard personnel as well as deciding on the employment of ship.

Regulation 7: Ship Security

Guidance is contained in sections 8, 9 and 13 of the ISPS Code.

Regulation 8: Ship Security Assessment (SSA)

This section specifies the requirements when a SSA is being conducted as well as what the SSA should entail. Company Security Officer (CSO) is held accountable for carrying out the SSA and is required to utilise expert assistance in the process. The Company Security Officer is mandated to acquire and record the required information for conducting an assessment. This section provides a list of the required information and details on the on-scene survey. The details of what should be considered part of the SSA are listed in this section and include:

- Each identified point of access should be examined in the SSA
- Significance of the current measures of security
- Persons, services, activities, and operations that it is essential to safeguard
- All possible threats
- All possible vulnerabilities[93]

[92] Ibid at Regulation 5 at 46-47.

Regulation 9: Ship Security Plan (SSP)

This is a comprehensive 11 page guideline on the Ship Security Plan. It begins with the preparation of the SSP, the various role players involved in the process of its submission for approval and most importantly the details that should be covered in the SSP.

The preparation and submission for approval of a SSP is the responsibility of the relevant CSO whilst the Administration provides guidance on the content and preparatory work of the SSP. All SSPs should detail the following:

- Organizational structure of security for ship
- Ships relationships with various roles players regarding security responsibilities such as Company, port facilities, relevant authorities and other ships
- Communication systems
- Basic security measures for security various levels
- Reporting procedures to the appropriate Contracting Governments[94]

This regulation further provides for details regarding each security level applicable, on the following:

- Organization and performance of ship security duties
- Access to the ship
- Restricted areas on the ship and what they may include
- Handling of cargo
- Delivery of ships stores
- Handling unaccompanied baggage
- Monitoring the Security of the Ship
- Differing security levels
- Activities not covered by the Code
- Declarations of security
- Audit and review

[93]Ibid at Regulation 8 at 48-52.
[94]Ibid at Regulation 9 at 52-63.

Regulation 10: Records

Records should be retained in any format with the objective of preventing unauthorised disclosure/access. This regulation stipulates that Contracting Governments duly authorised officers may access the records for purposes of authenticating the implementation of the ships security plans.[95]

Regulation 11: Company Security Officer

Direction is contained in sections 8, 9 and 13.

Regulation 12: Ship Security Officer

Direction is mentioned in sections 8, 9 and 13.

Regulation 13: Training, Drills and Exercises on Ship Security

This section details in a form of lists, the training requirements for the Ship Security Officer (SSO), Company Security Officer (CSO) and shore based Company personnel. It is comprehensive in outlining the specific training requirements for all relevant authorities/institutions.[96] The training includes the following:

- security administration
- international conventions
- Government legislation
- ship and port facility security measures
- techniques of conducting inspection, audits, monitoring and control

Regulation 14: Port Facility Security

Direction contained in section 15, 16 and 18.

Regulation 15: Port Facility Security Assessment (PFSA)

The relevant Contracting Government ought to provide approval for a completed PFSA whilst a RSO may conduct the PFSA. This regulation provides a list of elements that a PFSA should attend to within a port facility and it includes the physical security, procedural policies, utilities, structural integrity, radio and telecommunication systems.

[95] ISPS Code, Part B op cit n 39 at Regulation 10 at 63.
[96] Ibid at Regulation 13 at 64 -66.

Regulation 16: Port Facility Security Plan (PFSP)

This regulation is very detailed in its 14 page guidance on the Port Facility Security Plan. It begins with the preparatory stage of a PFSP, detailing the requirements of the plan and the details of what it should contain. It further elaborates on those accountable for the preparation of the plan as well as the Contracting Governments responsibilities in this regard.

The PFSO is accountable for the preparation of the PFSP and the content of each PFSP is customised according to the circumstance of each port facility. The Contracting Governments responsible for formulating advice on the content, preparing of a PFSP, developing techniques to measure the effectiveness of each PFSP and approving the PFSP.[97]

The PFSA will establish the necessity to appoint a PFSP and to formulate a PFSP as it contains amongst others the details of potential security risks and particular structures of the port facility that warrants the services of a PFSO. The PFSP will require for the appropriate security measures to be established and national security to be considered in order to minimise the probability of a security breach.

PFSPs should provide for:

- Detail security organization of the port facility
- Organisations associations with other relevant authorities
- Detail basic security level 1 in place
- Detail additional security measures of security level 2 and security level 3
- Consistent review, or PFSP audit
- Reporting procedures to appropriate Contracting Governments

Guidance is further provided on each security level requirements for various actions such as access to the facility of the port, cargo management, delivery of ships stores, restricted areas, unaccompanied baggage management and differing security levels.[98]

Regulation 17: Port Facility Security Officer

The Port Facility Security Officer should in exceptional circumstances assist when the Ship Security Officer has concerns relating to the validity of documents of identification of those

[97] Ibid at Regulation 16 at 71-85.
[98] ISPS Code, Part B op cit n 39 at Regulation 16 at 82-83.

that intend to board the ship for official purposes. [99] This Officer should not be accountable for routine confirmation of those intending to board the ship. Furthermore, sections 15, 16 and 18 provides the relevant guidance.

Regulation 18: Training Drills and Exercises on Port Facility Security

Regulation 18 firstly provides a very detailed list of 20 areas of training that the Port Facility Security Officer should receive training and be knowledgeable on security administration, methodologies for audits, inspection, control as well as monitoring, government legislation and regulations.

It secondly provides another list of 10 areas of training that the Port Facility personnel that have security responsibilities should receive training and be knowledgeable on some of the following: current security patterns and threats, security related communications, methods utilised to evade security processes, inspection, control, and monitoring techniques.[100]

Finally this regulation, has a section on drills, which should be conducted on a minimum basis of every three months and exercises with the objective of ensuring proficiency at all security levels for personnel of port facility, in all assigned security duties and to recognise security related deficiencies.[101]

Regulation 19: Verification and Certification for Ships

There is no further guidance provided in Part B. It can be deduced that this is so, since Part A, Regulation 19 is comprehensive in providing detailed guidelines on the process of verification and certification for ships.

Appendix 1: Form of a Declaration of Security between a Ship and a Port Facility (See Annexure 7).

Appendix 2: Form of a Statement of Compliance of a Port Facility (See Annexure 8).

[99] Ibid at Regulation 17 at 85.
[100] Ibid.
[101] Ibid.

2.7 *Conclusion*

The provisions of the ISPS Code create a platform for the international maritime community to be on the same level in terms of securing its ports, facilities and ships. Part A contains mandatory provisions whilst Part B contains specific guidelines for each regulation that may be utilised by states during the drafting stages of their own domestic maritime security legislations.

The application of the ISPS Code is of vital importance as it will enhance national and international security, as the security of the maritime environment is a transnational challenge, which requires regional and international efforts. Apart from providing protection against terrorists and other criminal acts, these new security measures, enhance the efficiency of the maritime industry by the:

- Reduction in delays
- Quicker processing times
- Improved asset control
- Reduced losses due to theft
- Decrease in insurance costs[102]

In conclusion the ISPS Code provisions are comprehensive in providing guidance on how to enhance maritime security. However it is essential that the process of implementation of these provisions is carried out in order to ensure that the shipping industry is protected and becomes efficient in its business processes.

[102]H Hesse and N L Charalambous op cit n 37 at 135.

CHAPTER 3: MARITIME SECURITY AND TERRORISM

3.1 *Introduction*

Since the 9/11 terrorist attacks, the concept of maritime security has expanded and maritime terrorism is recognised as a new threat to maritime security due to its blatant disregard of the generally accepted principle of freedom of the seas, impeding travel by sea, restricting the transportation of people and goods and the economic activities in various trading ports and sea routes around the world.[103]

It is internationally accepted that maritime terrorism is a transnational threat to international maritime trade. As such, the definitions of maritime terrorism utilised by different countries and organisations are similar, however each will classify the acts of terrorism according to their legislative definitions.[104] The United Nations defines maritime terrorism as "any action.....that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing any act."

Authors at the Corbett Centre for Maritime Policy Studies at the University of London identified two types of maritime terrorism namely: political and economic. Political maritime terrorism can be either carried out by the state or non-state organisations, whilst economic terrorism can be carried out with the use of violence such as human trafficking or without the use of violence such as the illegal transportation of contraband arms or drugs. [105]

Studies indicate that international maritime terrorism incidents are mainly as a result of the actions of terrorist groups that are recognised of having maritime capability, it include Al-Qaeda, Abu-Sayyaf, Al-Furqan and The Liberation Tigers of Tamil Eelam.[106]

This chapter discusses maritime terrorism on an international level relating to incidents before the implementation of the ISPS Code and after the implementation of the ISPS Code

[103] V Bezkorovainiy and S Sokolyuk 'Piracy, Maritime Terrorism and Disorder at Sea' (2012) Corbett Paper No 8 at *The Corbett Centre for Maritime Studies* at 4 available at http://www.kcl.ac.uk/sspp/departments/dsd/research/researchgroups/corbett/corbettpaper8.pdf (accessed on 03 July 2015).
[104] A Mazaheri 'How ISPS Code affects Ports and Port Activities' (2008), a Thesis submitted to the *University College of Boras in Sweden* at 8 available at (accessed on 15 July 2015).
[105] V Bezkorovainiy and S Sokolyuk op cit n 103 at 16-17.
[106] Ibid.

in order to evaluate the success of the ISPS Code. The evidence is strong and it will illustrate that the ISPS Code is beneficial to the security of the maritime environment.

3.2 *International Maritime Terrorism Incidents: Before the ISPS Code*

Maritime history recorded one of its first acts of terrorism in 1961[107] however only in October 1985, with the Italian cruise ship Achille Lauro being hijacked, did the international maritime community react with preventative measures. The IMO responded to this incident with the Resolution A.584 (14), which are measures to prevent unlawful acts that threaten the security of passengers and crew as well as the safety of ships. IMO also issued in 1986 Circ.443 on measures to prevent unlawful acts against passengers and crew on board ships.[108] Shortly afterward, the IMO developed and adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA). This Convention provides that the appropriate action is instituted against those persons who commit acts of unlawfulness against ships.[109]

In addition during 1986, a study regarding maritime terrorism was requested by the UN General Assembly. The outcome of the study resulted in the IMO adopting MSC/Circ. 443 which were recommendations on measures to prevent unlawful acts against crew and passengers on board vessels. These measures became the foundation for the development of the ISPS Code.[110]

The IMO held a Diplomatic Conference in December 2002, focusing on the prevention and suppression of acts of maritime terrorism and identifying methods of enhancing global maritime security. During this conference, a number of amendments were adopted to the SOLAS Convention, including the ISPS Code, the additional requirements for ships to standardise ship identification markings, fit Automatic Identification Systems (AIS) and to carry on board a Continuous Synopsis Record (CSR).[111]

---

[107] L Joubert op cit 1.
[108] H Hesse and N L Charalambous op cit n 37 at 124.
[109] C Trelawny op cit n 50.
[110] P Hellberg op cit n 48.
[111] F McNaught 'Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the Maritime Security Threat' (2005) *Geddes Paper* 91.

Pre-9/11

1961: Santa Maria - On 23 January 1961, a 609 foot long, 20,900 ton Portuguese luxury cruise liner with 600 passengers and 300 crew on board was seized and controlled by a group of 24 members of the Portuguese and Spanish opposition movement who had boarded the ship with weapons hidden in their luggage. The opposition movement members eventually surrendered to the Brazilian authorities and were granted political asylum.[112]

1973: Sounion - In March 1973, in Lebanon, a Greek passenger ship Sounion sank in the Beirut port. Whilst the ship was docked, the Palestinian terrorists, attached a limpet mine to the hull of the ship. The terrorist planned on blowing up the ship once it was at sea however due to Swedish intelligence, the departure was delayed in order to allow for the passengers on board to disembark and thereafter the ship sank alongside the berth.[113]

1985: Achille Lauro - On 7 October 1985, the Italian liner Achille Lauro, while sailing from Alexandria to Ashdod, Israel was hijacked by four men who were part of the Palestine Liberation Front (PLF), this incident was recorded as one of the first terrorist acts in maritime history.[114]

1985: Rainbow Warrior – In July 1985, the Greenpeace ship was moored in New Zealand, preparing to confront French nuclear testing in the Moruroa Atoll[115] when two explosions ripped through its hull, killing one crew member.[116] The two explosions was as a result of two bombs planted by the French Secret Service agents.[117]

The response received from the international community on maritime terrorism was reflected in the IMO adopting the 1988 Rome Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), and the 1988 Rome Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the

[112]D Bryant 'Hijacking of the SS Santa Maria' (2011) Maritime Professional available at http://www.maritimeprofessional.com/blogs/post/hijacking-of-the-ss-santa-maria-13422War II (accessed on 30 June 2015).
[113] L H Bergqvist 'The ISPS Code and Maritime Terrorism' (2014) available at http://cimsec.org/isps-code-maritime-terrorism (accessed on 15 April 2015).
[114] L Joubert op cit n 1 at 118-119.
[115] The bombing of Rainbow Warrior at http://www.greenpeace.org/international/en/about/history/the-bombing-of-the-rainbow-war/.
[116] Nuclear free New Zealand at http://www.nzhistory.net.nz/politics/nuclear-free-new-zealand/rainbow-warrior.
[117] The bombing of Rainbow Warrior op cit n 115.

Continental Shelf.[118] The SUA Convention was intended to ensure that responsible authorities are able to extradite or prosecute persons responsible for committing terrorist acts at sea.[119]

1990: The Tamil Tigers Acts of Maritime Terrorism - The Liberation Tigers of Tamil Eelam with the Sea Tigers brigade[120] was involved in maritime terrorism during the civil war period between the Sri Lankan government and the Tamil Tigers.[121] The Liberation Tigers of Tamil Eelam has since July 1990 been involved in over 40 maritime terrorism attacks.[122]

Post 9/11

2000: USS Cole - On 12 October 2000, the US Navy vessel, Cole, while refuelling at a port in Aden, Yemen, was attacked by two suicide bombers navigating a small motor boat full of explosives. This incident resulted in the death of 17 crew members whilst 39 others were injured. An Al-Qaeda supported terrorist group claimed responsibility for the attack.[123]

2002: Limburg - In October 2002, the French owned crude oil tanker, the MV Limburg was reported by BBC as carrying 397 000 barrels of crude oil and was attacked by Al-Qaeda suicide bombers whilst in Yemen. An explosive-laden boat struck tanker's hull which resulted in an explosion killing one crew member, injuring 12 people and spilling 100 000 barrels of oil. A Saudi national admitted to his involvement in the attacks and pleaded guilty to charges of terrorism. He confirmed that he underwent training to execute the attack in an Al-Qaeda training camp.[124]

2004: Superferry 14 - In February 2004, a Philippines ferry was attacked by the Abu-Sayyaf terrorist group which resulted in the death of 116 persons. The explosion resulted from a

---

[118] D C Turack 'Maritime Terrorism and International Law' (1992) 41 (2) *The International and Comparative Law Quarterly* at 490.

[119]C Joyner 'Navigating Troubled Waters: Somalia, Piracy, and Maritime Terrorism' (2009) 10 (2) *Georgetown Journal of International Affairs* at 83.

[120] The Sea Tigers brigade was suspected of being involved in several hijacking incidents of vessels in waters off the coast of Sri Lanka. These incidents includes: 1995 -Irish Mona, 1996- Princess Wave, 1997- Athena, Misen, Morong Bong, MV Cordiality and 1998-Princess Kash and Silk Pride.

[121] L H Bergqvist op cit 113 at 2.

[122] C Z Raymond 'Maritime Terrorism in Southeast Asia: Risk Assessment' (2005) 75 *Institute of Defence and Strategic Studies Singapore* at 4.

[123]E S Nelson 'Maritime Terrorism and Piracy: Existing and Potential Threats' (2012) 3(1) *Global Security Studies* at 20.

[124]'Guantanamo Prisoner Al-Darbi Admits MV Limburg Attack' (2014) *BBC News* available at http://www.bbc.com/news/world-us-canada-26277556 (accessed on 30 June 2015).

hidden television set in the vessel that contained a 4 kilogram TNT time bomb.[125] This incident is considered the most serious act of maritime terrorism due to the number of deaths that resulted from this attack.[126]

As outlined in a paper by Bezkorovainiy and Sokolyuk dated 2012, a number of distinctive characteristics emanate from all these incidents of international maritime terrorism:

- Trained concurring crew members are used for conducting maritime terrorist attacks;
- Valuable and hi-tech weaponry such as the long-range weapons and explosives are used;
- Criminals carrying out the act of maritime terrorism are part of larger notorious grouping/maritime terrorist group.[127]

These incidents of maritime terrorism display the potential susceptibility of maritime vessels to terrorist attacks. The catastrophe of the 9/11 terrorist attacks caused the international maritime society to realise the possibility of a vessels loaded with weapons of mass destruction being used to attack critical infrastructure such as port facilities, harbours and other vessels. [128] In view of such threats, anti-terrorism regulations such as the ISPS Code were introduced for implementation by states in order to provide protection to their vessels and port facility and enhance maritime security globally.

3.3 *International Maritime Terrorism Incidents: After the ISPS Code*

2005: Don Ramon – An Al-Qaeda linked group of terrorist attacked a passenger ship in Filipino waters. They placed a time bomb in the ship's galley, beneath gas cylinders, this explosion resulted in the sinking of the ship and 30 injured passengers.[129]

2010: M Star - In July 2010, the Japanese oil tanker M Star in the Strait of Hormuz was attacked using explosives to damage the hull of the vessel. Two days later, the Brigades of Abdullah Azzam, an Al-Qaeda linked militant group claimed responsibility for the attack.[130]

[125] 'Superferry 14 Fire leaves 116 dead' (2014) available at www.terrorism.com/2014/04/23/superferry-14-fires-leaves-116-dead/ (accessed on 01 July 2015).
[126] S Bateman 'Assessing the Threat of Maritime Terrorism: Issues for the Asia-Pacific Region' (2006) 12(3) at 81.
[127] V Bezkorovainiy and S Sokolyuk op cit n 103 at 18.
[128] A Mazaheri op cit n 104 at 7.
[129] V Bezkorovainiy and S Sokolyuk op cit n 103 at 3.

2013: Cosco Asia - In September 2013, a Chinese owned vessel was attacked with a rocket propelled grenade while on transit in the Suez Canal as reported by Turkey Sea News. [131] An Islamist group Al-Furqan claimed accountability for this attack.[132] Fortunately, the attack resulted in minor damages to the vessel and no casualties, this attack was on a small scale, however, due to the economic importance of the Suez Canal, the Egyptian Government plans to increase its security by building a protective wall along the Canal. [133]

3.4 *Increasing security levels of the ISPS Code*

Evidence that the protective framework and guidelines offered by the ISPS Code is being globally utilised by states for the protection of their vessels against acts of terrorism can be seen in an increase in the ISPS security levels by various states in order to counter threats of potential terrorist attacks. Notably, in August 2013, the United Kingdom increased its ISPS security level from Level 1 to Level 3 for all British flagged ships in the territorial waters of Yemen due to an increase in Al-Qaeda attacks; during June – July 2013, pre-empting possible terrorist attacks, the Indian government raised its security level at some ports to Level 2.[134]

The international maritime community recognises maritime terrorism as a rapidly growing threat to global maritime security and various international initiatives are underway to enhance maritime security. As such, partner states of the Five Power Defence Arrangements (FPDA), which includes New Zealand, Singapore, United Kingdom, Australia and Malaysia agreed to include maritime terrorism as a security threat in their military exercises.[135]

---

[130] Oman 'Al-Qaeda link confirmed for M Star VLCC Attack' (2010) from Seatrade Maritime News available at www.seatrade-maritime.com/news/asia/al-Qaeda-link-confirmed-for-M-Star-VLCC-attack.html (accessed on 03 July 2015).

[131] SeaNews Turkey article 'Fire, explosion aboard 10,061-TEU Cosco Asia in Suez terror attack' *International Shipping Magazine* available at http://www.seanews.com.tr/news/110977/Fire-explosion-aboard-10-061-TEU-Cosco-Asia-in-Suez-terror-attack-.html accessed on (02 July 2015). The authority of Suez Canal made a statement that the aim of the attack was to disrupt the flow of vessels through the canal.

[132] D Barnett 'Al-Furqan Brigades claims two attacks on ships in Suez Canal, threaten more' (2013) *A blog of the long war Journal* (accessed on 28 May 2015).

[133] V Bezkorovainiy and S Sokolyuk op cit n 103 at 11.

[134] Ibid.

[135] C Z Raymond op cit n 122 at 20.

3.5 *Conclusion*

Research indicates that due to the implementation of the ISPS code, there has been an increase in the awareness and implementation of maritime safety and security measures by member states. There has also been a decrease in reported incidents of serious acts of maritime terrorism in the last ten years.[136] These positive outcomes stemming from the implementation of the ISPS Code is evidence of its success in fulfilling its objectives.[137] As stated by Author Lars H. Bergqvist, Swedish Master Mariner and a Reserve Officer in the Royal Swedish Navy - "the Code is now an accepted part of shipping, and the advantages are being appreciated." [138]

[136] L Joubert op cit n 1 at 131.
[137] L H Bergqvist op cit n 113.
[138] Ibid.

CHAPTER 4: IMPLEMENTATION AND IMPACT OF THE ISPS CODE

4.1 *Introduction*

South Africa continues to be the largest economy on the continent[139] and in order to maintain this status it is key to ensure the efficiency of the ports. Maintaining the ISPS Code is of utmost importance as it safeguards that foreign trade relations are maintained and this ensures the growth of the South African economy. As stated by the CEO of Transnet National Port Authority "The efficient running of ports is important to the well-being of the economy of South Africa."[140]

This chapter will illustrate the implementation of the ISPS Code in South Africa, evaluate the implications/risks of non-compliance and how South African ports mitigate these risks. Thereafter a mini comparative study will illustrate the implementation of the ISPS Code in various other signatory countries to SOLAS such as Sweden, Singapore, Iran, United Kingdom, Cyprus, and Germany in order to determine its impact. The core question of whether the ISPS Code has fulfilled its purpose will be answered together with recommendations for IMO to improve its mandate of maritime security.

4.2 *Implementation of the ISPS Code in South Africa*

South Africa, being signatory to the IMO, ratified the ISPS Code and implemented its provisions via the Merchant Shipping (Maritime Security) Regulations 2004, hereafter referred to Regulations 2004.[141] All eight main commercial ports in South Africa namely Richard Bay, Durban, East London, Port Elizabeth, Mossel Bay, Saldanha Bay, Ngqura and Cape Town[142] are in compliance with Regulations 2004 and the ISPS Code since 29 June 2004.[143]

---

[139] Dr A Maharaj 'Economic Development Position Paper on Port Expansion' 2013 available at www.durban.gov.za (accessed on 10 February 2016).

[140] S Gama, CEO of TNPA presentation "BEE at the National Ports Authority of South Africa" (2004) available at www.transnetnationalportauthority.net (*accessed on 26 January 2016*).

[141] Transnet National Port Authority op cit n 14.

[142] South African Maritime Safety Authority, Marine Notice No.12 of 2008, The Merchant Shipping (Maritime Security) Regulations, 2004, section 1. Marine notice providing guidance to the industry on the application of the Merchant Shipping (Maritime Security) Regulations, 2004 and the International Ship and Port Facility Security Code.

[143] Transnet news available at http://www.transnetnationalportsauthority.net/Port%20Operations/Pages/Security.aspx (accessed on 29 July 2015).

The designated authority[144] for the administration of maritime security in South Africa is the South African Maritime Safety Authority (SAMSA),[145] which is responsible for:

- Approval of Ship Security Plans
- Verification of compliance with plans
- Issuing the International Ship Security Certificate (ISSC)
- Issuing the Continuous Synopsis Record (CSR)[146]

SAMSA is further mandated in terms of section 2 of the SAMSA Act 5, to give effect to various legislation relating to the maritime environment and it includes: The Merchant Shipping Act, Marine Traffic Act and the Ship Registration Act, 1998. Additionally, when necessary, SAMSA issues marine notices[147] with the aim of providing guidance to the industry on the application of the Merchant Shipping (Maritime Security) Regulations 2004 and the ISPS Code.

4.2.1 *Merchant Shipping (Maritime Security) Regulation 2004*

To obtain a better understanding of the provisions of Regulations 2004, there will be an analysis of the breakdown of the functionality of certain provisions of Regulations 2004, identification of the risks that would emerge as a result of non-compliance and control methods adopted at the South African ports to mitigate the risks.

Part 1: Preliminary

Section 5: Unlawful interference with maritime transport[148]

The non-compliance of this provision of unlawful interference with maritime transport may result in South Africa losing its credibility in two-ways. Firstly in-terms of the ISPS Code and secondly with regard to bi-lateral trading agreements which would lead to financial loss.[149] Should this occur, South African ports would be considered as high risk ports and foreign

[144] ISPS Code, Part A op cit n 12 at section 4.2 at 36.
[145] SAMSA was established on 01 April 1998 under the SAMSA Act 5 of 1998, the objectives of the Authority are to ensure safety of life and property at sea, prevent and combat pollution from ships in the marine environment and promote the Republic's maritime interest. This is according to the SAMSA Act 5 of 1998, Objectives at 8.
[146]SAMSA Marine Notice 12 of 2008 and the Merchant Shipping (Maritime Security) Regulations, 2004.
[147] An example would be the Marine Notice No.12 of 2008 which provides the maritime industry with guidance on the application of the Merchant Shipping (Maritime Security) Regulations, 2004 and the ISPS Code. Specific guidance is provided on various maritime security related matters including: Certification of South African Ships, Security Level in South African Territorial Waters and Port Security.
[148] Merchant Shipping (Maritime Security) Regulations 2004, Section 5 at 13.
[149] TNPA Compliance Control Plan for the Maritime Security Regulations 2013, Division 5 at 1.

vessels would be reluctant to engage in the business at these ports.[150] This situation would ultimately become detrimental to the growth of the economy of the country as the efficient running of the ports is vital to the economy of South Africa.[151]

In an effort to maintain the ISPS Code status and mitigate the risks posed by non-compliance of this provision, South African ports implement strict control measures within designated port limits, and on land all port users using the marine environment are searched, and their purpose of visits are verified.[152] Then on the land side, Border Police conducts coastal and waterfront patrols in an effort to provide safe seas, and prevent piracy.[153]

Section 13: Complying with Security Directions

Non-compliance with security directions may result in the compromising of the ISPS Code status of the Ports in South Africa. To retain South Africa's status and be regarded as a safe port to conduct business, before a vessel docks, the Port Security Manager establishes through the Department of Transport that a vessel has obtained clearance.[154]

Part 2: Maritime Security Levels and Security Directions

Sections 16, 17 & 18: Security level 1 applies to South Africa's eight main commercial ports.[155] Any change in security levels must be declared by the Director General for Transport and will it be notified by Notices to Mariners, Navigational Warning and Marine Notices.[156] The Director General for Transport is required to consult with National Intelligence Co-ordinating Committee (NICOC) prior to making a declaration of a change in security level.[157]

In order to ensure compliance with the provisions of Part 2 as well as maintaining the ISPS Code status and to be regarded as a safe port, there is constant communication with the Department of Transport for the verification that vessels have been granted clearance. This

[150] Ibid
[151] S Gama op cit n 140.
[152] TNPA Compliance Control Plan op cit n 149 at Division 5 at 1.
[153] Ibid at Division 5 at 1.
[154] Ibid at Division 5 at 1.
[155] Merchant Shipping (Maritime Security) Regulations op cit n 148 at Division 1, Section 16 at 16.
[156]SAMSA Marine Notice 12 of 2008 op cit n 146.
[157] Merchant Shipping (Maritime Security) Regulations op cit 148 at Section 5 at Section 18 at 16.

verification ensures that the vessels that are docking are safe and does not pose any risk to other vessels and the port so that the security level declared is maintained.[158]

Section 23: Notifying maritime security level 2 and 3 declarations and revocations[159]

The risk of non-compliance to this provision would be a definite loss of business from maritime participants from foreign countries as their vessels may be compromised due to the failure to notify them on the change of levels of security.[160] In order to mitigate this risk of non-compliance and in an effort to maintain trading relations with foreign countries, ports in South Africa liaise with all port users about any change in the levels of security.[161] This provision is important as non-compliance will also damage the reputation of South Africa; therefore should a port operator fail to comply with this provision, the port operator will be committing an offence and will be either liable for a fine or will be imprisoned.[162]

In addition, for vessels that seek information on maritime security and for vessels that are arriving on the South African coast, there is a National Contact Point for their usage, namely the Maritime Rescue Co-ordination Centre (MRCC) which is situated in Cape Town.[163]

Part 3: Maritime Security Plans

According to Section 39, there is an obligation for the maritime industry participants i.e. port service providers, port operators and port facility operators to have a security plan which should be revised every five years.[164] These security plans together with an attached security risk assessment is required to be submitted to the Department of Transport for review and its approval.[165] Non-compliance with this provision, that is, failure of maritime participants having security plans is an offence which is punishable by a fine or imprisonment not exceeding 12 months.[166]

[158] TNPA Compliance Control Plan op cit n 149 at Division 5.at Section 17 at 2.
[159] Merchant Shipping (Maritime Security) Regulations op cit n 148 at Section 5 at 19.
[160] TNPA Compliance Control Plan op cit n 149 at Division 5 at Section 23 at 3.
[161] Ibid at 3.
[162] Merchant Shipping (Maritime Security) Regulations op cit n 148 at 2004, Section 5 at 18.
[163] Article on General Information for South Africa, Section- ISPS Compliance available at http://www.findaport.com/country/south-africa (accessed on 28 May 2015).
[164] Merchant Shipping (Maritime Security) Regulations op cit n 148 at Section 5 at sections 39, 40 and 53 at 24 and 29.
[165] Ibid at section 47 at 27.
[166] Ibid at section 40 at 24.

Part 4: Ship Security Plans and International Ship Security Certificates

It is a requirement according to Section 57 of Regulations 2004 that all South African regulated ships have a Ship Security Plan and an International Ship Security Certificate. Section 62 provides the requirements of a Ship Security Plan and it must include:

- A Ship Security Assessment.
- Security measures that is to be applied according to the security level of the ship.
- Ship Security Officers details.

Further detailed guideline for the development of the Ship Security Plan is contained in Section 63 of the Regulations. Compliance to this provision is vital as failure to comply is an offence which is punishable.[167] Furthermore the plan is required to be revised every five years.[168] The Transnet Maritime School of Excellence provides maritime training to the maritime personnel in South Africa on the compilation of the Ship Security Plan.

Part 5: Foreign Regulated Ships

Section 85 of the Regulations places an obligation on foreign-regulated ship to obtain an International Ship Security Certificate (ISSC) or its equivalent as well as to carry on board the vessel its ship security records. Furthermore foreign regulated ships are required to:

- Provide pre-arrival information[169] so that the vessel obtains clearance.
- Allow for inspections to be carried out on the vessel[170] to mitigate the risk of a maritime threat.
- Comply with security levels[171] to maintain South Africa's declared security levels.

Part 6: Powers of Officials

This section provides a list of authorised officers, namely: surveyor, proper officer, member designated by the Director General (Department of Transport, The State Security Agency, the South African Defence Force and the South African Police Service).[172] These authorised

[167] Merchant Shipping (Maritime Security) Regulations op cit n 148 at Section 5 at Section 59 at 31.
[168] Ibid at section 71 at 35.
[169] Ibid at section 86 at 40.
[170] Merchant Shipping (Maritime Security) Regulations op cit n 148 at section 87 at 41.
[171] Ibid at section 88 at 41.
[172] Ibid at section 97 at 50.

officers are provided with a list of duties to perform in order of ensuring compliance with this regulation, these duties include:[173]

- Inspection of the vessel, its records and other documentation[174]
- Photograph and inspect equipment in the ship, the ship security record and other documents[175]

The emerging risk of non-compliance of sections 98 and 99 would result in conflict of interest within government departments involved and this may result in operational disruptions in the ports.[176] South African, ports in an effort to prevent such risks, have the roles of the government departments clearly defined and implemented during their monthly Border Control Operational Coordinating Committee (BCOCC).[177]

Part 7: Reporting Maritime Transport Security Incidents

Section 103 explains that a maritime transport security incident may be defined as a threat of unlawful interference/an unlawful interference with maritime transport. A list is provided on the persons responsible for reporting security incidents, such persons include: port facility operators, ship operators, ship masters, port operators, and employees of the maritime industry participants.[178] It is further an offence to not report maritime transport security incidents.[179]

The failure to report incidents as required by this provision may result in the compromising of the status of the ISPS Code and security of the ports which will negatively impact on the business. South African ports mitigate this risk by implementing a requirement that the Port Facility Security Officer is mandated to report incidents within 24 hours. In addition the monthly engagements of the BCOCC further addresses the security incidents reported.[180]

[173] Merchant Shipping (Maritime Security) Regulations op cit n 148 at Section 5 at section 98 at 51.
[174] Ibid at section 98 at 51.
[175] Ibid at section 99 at 51.
[176] TNPA Compliance Control Plan op cit n 149 at 9
[177] The BCOCC mandate is to strategically manage the borders of South Africa. It comprises of the departments of Home Affairs, South African Revenue Services, State Security Agency, Public Works, Health, Defence, South African Police Services, and Agriculture. Details available at http://www.borders.sars.gov.za/, (accessed on 28 November 2015).
[178] Merchant Shipping (Maritime Security) Regulations op cit n 148 at sections 104-107 at 53 and 54.
[179] Ibid at sections 108 at 55.
[180] TNPA Compliance Control Plan op cit n 149 at 10 and 11.

Part 8: Information-gathering

The Director General may require security compliance information in writing, orally or by electronic means, which should be forth-coming from those requested.[181] Any refusal without a good reason, supplying of false or misleading information will amount to an offence which is punishable by either a fine or imprisonment.[182] The risk of providing false information will result in reputational damage to South Africa and threaten the status of the ISPS Code. South Africa ports have mitigated this risk by stating that non-compliance is an offence which is punishable.

4.3 *The Impact of the ISPS Code in South Africa*

According to Transnet National Port Authority, a division of Transnet SOC Ltd there has been both a positive impact as well as a negative impact of the application of the ISPS Code on specifically port operations.[183]

Positive impact on port operations:

- Consistency in maritime security as the Security policies and measures procedures have been standardised with the requirements in Regulations 2004.
- The handling of the vessel clearance process has been improved.
- A decrease in the crime rate at the ports with the increase in security measures and restricted access policy being implemented.
- Improvement in the collaboration between Port/Facility Security and State Security/Emergency Agencies/Services.[184]

Negative impact on port operations:

- Vessel clearances delays.
- Traffic congestions into and out of the Port/ Facility entrance points, specifically on uncertainty regarding privately-owned port facilities as well as some resistance in terms of co-operation with measures procedures and security policies. However South Africa mitigates these challenges in the SA Maritime Transport Security Bill.[185]

[181] Merchant Shipping (Maritime Security) Regulations op cit n 148 at section 116 at 59.
[182] Ibid at section 116(5) at 59.
[183] TNPA Presentation on *Status Report on Port Security in South Africa* - 2009 available on website of Port Management Association of Eastern and Southern Africa http://www.pmaesa.org (accessed on 17 April 2015).
[184]Ibid at slide 13.
[185] Ibid

Identified short coming in the ISPS Code:

- The ISPS Code is limited in terms of its application of vessels[186], it is not applicable to fishing vessels, and government owned or operated vessels or vessels engaged exclusively in local trade within one state.[187]

Transnet National Port Authority, specifically the Compliance Division creates a Compliance Control Plan which is a document stipulating each provision in Merchant Shipping (Maritime Security) Regulation, the risk of non-compliance to the provision and the control measures in place to mitigate the risks. These security measures ensures that South African ports maintains their ISPS Code status and is regarded as a safe port.[188]

4.4 *Impact of the ISPS Code on other Signatories to the SOLAS Convention*

Below is a brief discussion on the impact studies undertaken by various jurisdictions. The results are categorised as positive/strengths and negative/weakness/shortcomings experienced in the implementation of the ISPS Code within these jurisdictions. Some countries like Singapore and the United Nations have not only identified the weaknesses but has taken the initiative to address the identified weaknesses.

4.4.1 *Sweden*

Sweden's maritime administration requested for research to be conducted in 2009 to evaluate the impact of the implementation of the ISPS Code. This research comprised of questionnaires/surveys and interviews with questions relating to amongst others the advantages and disadvantages of the application of the ISPS Code and it was provided to maritime stakeholders, the shipping industry as well as the maritime administration for a response.[189] The results of the research indicated the following:

Positive impact of the ISPS Code

- Increased maritime security on-board ships as a result of access control measures in place.
- Enhanced knowledge and increased awareness and understanding due to the increase in number of training and drills sessions on-board.

[186] See Regulation 3 of the Part A of the ISPS Code.
[187] C Forrest op cit n 24 at 14.
[188] Interview with a member of Transnet National Port Authority at the Port of Durban on 07 January 2016.
[189] P Hellberg, op cit n 48 at 54.

- Increase in safety and security of personnel and maritime environment as the incidents of theft and damage to property were decreased due to the strict access control measures implemented.[190]

Negative impact of the ISPS Code

- Ships were delayed due to their suppliers experiencing challenges during the security checks at the access points.
- Financial impact as delays resulted in extra costs.[191]

4.4.2 *Singapore*

Port of Singapore Authority (PSA) Singapore is considered to be one of the busiest ports in the world and in the year 2014 it has been recognised to have cumulatively handled 500 million TEUs, which is a significant milestone as it is the first port in the world to have achieved this accolade.[192] Singapore's application of the ISPS Code is described as "one of the success stories" as its container ships were certified as ISPS compliant prior to the deadline, and its ships and port facilities conformed to the ISPS Code requirements by 01 July 2004.[193]

In assessing the effectiveness of the ISPS Code in Singapore, the Geddes Paper[194] identified the restriction of the applicability of certain vessels types as a weakness of the ISPS Code, that its non-application to many vessels, can be exploited by terrorists.[195]

The strengths of the ISPS Code, identified in this research paper include:

- The consistent approach utilised internationally regarding maritime security.
- The mandatory Part A of the ISPS Code.
- Cost savings from the reduction of pilferage and incidents of theft.[196]

Singapore implemented several of its supplementary security initiatives aimed at addressing the weakness of the ISPS Code i.e. only applicable to certain types of vessels. One such

[190] Ibid at 62.
[191] Ibid at 62.
[192] PSA Singapore op cit n 12.
[193] CZ Raymond 'The Challenge of Improving Maritime Security: An Assessment of the Implementation of the ISPS Code and Initial Responses as to its Effectiveness'(2004) Institute of Defence and Strategic Studies Commentaries Singapore 62/2004 2 available at www.idss.edu.sg (accessed on 29 July 2015).
[194] F McNaught op cit n 111.
[195] Ibid at 93.
[196] Ibid at 94.

initiative is a 'Ship Self-Security Assessment Checklist' which small vessels (excluded from the ISPS Code) are mandated to complete and keep a copy on-board before actually entering the Singapore port waters.[197] Another initiative is that of a Harbour Craft Security Code (HCSC) which mandates harbour craft to comply with general security standards.[198] The HCSC comprises of practical security measures such as a prerequisite of the Master of a harbour craft to make entries in the Harbour Craft Log when conducting business and retain the log on-board for a minimum time of 3 months.[199] These supplementary security initiatives have been implemented by the Singapore port authority in an effort to mitigate the risk posed by the restriction of the vessel type.

4.4.3 *Iran*

The ISPS Code, has been successful as an anti-terrorism regulating mechanism, this is according to an empirical study conducted on the outcome of the implementation of the ISPS Code on the ports of Iran, in the area of Abadan, [200]

This research concluded that the positive impacts of the ISPS Code include:

- More accurate documentation as there are integrated standards for documents.
- Increase in safety and security.
- Lower danger risk.
- Less incidents of smuggling and theft.
- Improved control of cargo circulation, personnel and port area.
- A more secure and safe working environment[201]

Whilst the negative impact of the ISPS Code include:

- Slow work progress.
- Increase in administration costs and paperwork
- Various interpretations of the ISPS Code was identified as a weakness.[202]

[197] Maritime Port Authority of Singapore op cit n 12. This Ship Self-Security Assessment Checklist purpose is to benefit security of the crew and ship and to further ensure port is ready and prepared in terms of security for the entrance of small vessels.
[198] CZ Raymond op cit n 193.
[199] PSA Singapore website, available at https://www.singaporepsa.com/ (accessed on 15 January 2016).
[200] S N Saeedi, S Khodakhshi, H Jafari, 'An Empirical Study on Effects of ISPS Code Implementation on Iran's Port Activities' (2012) ISSN 2322-2360 (7) available at www.universalrg.org (accessed on 08 August 2015).
[201] Ibid at 2359.
[202] S N Saeedi, S Khodakhshi, H Jafari, op cit n 200 at 2359.

4.4.4 *United Kingdom, Cyprus, Germany, Norway and the Netherlands*

Research conducted by Burmester at the United Kingdom Institute of Higher Education in Southampton on the application of the ISPS Code in the United Kingdom, Cyprus, Germany, Norway and the Netherlands indicated that much has been accomplished in terms of the objectives of the ISPS Code.[203]

However the following are some common shortcomings that were identified:

- The various interpretations of the ISPS Code requirements.
- Pre-arrival notifications need to be standardised.
- Increase in paperwork.
- Financial support required.
- Exclusion of ships under 500gt.
- Training should be clearly defined as well as included into the Standard Training Certification and Watchkeeping (STCW 95) requirements in order to circumvent duplication of training.[204]

4.4.5 *United Nations Conference on Trade and Development (UNCTAD) Survey*

The United Nations Conference on Trade and Development (UNCTAD) in 2007 conducted a compliance and impact study on the ISPS Code in the form of a global survey with the following objectives:

- Establishment of the order and range of magnitude of the ISPS Code-related expenditures.
- Clarification of the implementation process and the level of compliance.[205]

[203] C Burmester "International Ship and Port Facility Security (ISPS) Code – Perceptions and Reality of Shorebased and sea-going staff' (2004) at 6 Southampton Institute of Higher Education, United Kingdom.
[204] Ibid.
[205] United Nations Conference on Trade and Development 'Maritime Security: ISPS Code Implementation, Costs and related Financing' (2007) UNCTAD Secretariat at 5 available at http://unctad.org/en/Docs/sdtetlb20071_en.pdf (*accessed on 15 June 2015*).

The outcome of the survey indicates the objectives of the ISPS Code has been accepted as legitimate by both the respondent ports and governments and there has been a general positive impression of the new security regime.[206]

- Improved business practices
- Standardising risk assessment
- Increased awareness
- ICT usage and crime reduction
- Streamlining processes[207]

The survey further indicates that the financial implications for implementing the ISPS Code vary between larger and smaller ports. To assist with financing, cooperation and partnership initiatives should be reinforced, such as technical assistance, financial support, capacity building, exchanging information.[208] Developing countries can be assisted through bilateral and regional arrangements as well IMO instruments such as the International Maritime Security Trust Fund[209] and Integrated Technical Co-operation Programme.

4.5 *International Maritime Organisation (IMO) Research Findings*

The International Maritime Organization (IMO) has announced a "high degree of compliance" with the ISPS Code.[210] Its reports indicated that the Contracting Governments had approved 97% of declared port facilities.[211] In addition 89% of over 9000 declared port facilities have approved Port Facility Plans whilst 90% of ships that are obligated to be in compliance with the ISPS Code have been issued with their International Ship Security Certificates.[212] These Member States have with their designated authority implemented the ISPS Code via their domestic legislation.

---

[206] Ibid.
[207] Ibid.
[208] Ibid at 41.
[209]Established in June 2003 to assist IMO to respond to requests for technical assistance on issues of maritime security, various governments contribute to the Fund including: United States, United Kingdom, Egypt, Denmark, the Russian Federation, and Germany.
[210] International Maritime Organization IMO: Security compliance shows continued improvement. *Latest Press Briefing* on August 6, 2004, available at http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3760 (accessed on 29 July 2016).
[211] F McNaught op cit n 111.
[212] CZ Raymond op cit n 193 at 2. Statistics also available at International Maritime Organization IMO: Security compliance shows continued improvement. Latest Press Briefing on August 6, 2004, available at (http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3760 (accessed on 29 July 2015).

Specific focus is given to the IMO, due to the significant role it has played in the maritime industry and the direction it provides to the international maritime community. In addition a number of knowledgeable persons on the maritime security environment from the IMO have conducted research and assessments relating to the ISPS Code and its impact on the international maritime community. This section will focus on two papers written by prominent members of the IMO, the first paper (Senior Deputy Director Captain Hartmut G. Hesse) is research with the focus on the impact of the international communities in relation to the implementation of the ISPS Code, whilst the second paper (IMO Safety Division authors, Hesse and Charalambous) focuses on the IMO findings of global issues that has resulted from the application of the ISPS Code. These papers view of the ISPS Code is on a practical level and focus is made on the impact of its implementation on the maritime environment and the impact on the IMO. These are the critical areas of impact that are needed in order to assess whether the ISPS Code has fulfilled its purpose. In essence it will be showed that the ISPS Code plays a dual role of providing protection against terrorist activities and enhancing the efficiency of the maritime industry.

4.5.1 *IMO identifies Global Issues in Maritime Security*

Global issues in maritime security have been identified in an Implementation Assessment of the ISPS Code conducted by the Senior Deputy Director Captain Hartmut G. Hesse from the Maritime Safety Division of IMO. The outcome of the Assessment indicated:

Inadequacies:

- IMO has been provided with inaccurate or incomplete data.
- Guidance material provided by IMO is not being utilised completely.
- There are no provisions to evaluate the continued effectiveness of measures implemented.[213]

Inconsistency:

- The methodology in setting security levels.
- The port facilities definition.
- Providing training that is related to security.

[213] HG Hesse '3 years on –What are the Global Issues in Maritime Security' (2007) available at www.imo.org/en/KnowledgeCentre/InformationResourcesOnCurrentTopic/MaritimeSecurity and ISPSCode/Documents/Information%20Resources%20on%20MARITIME%20SECURITY%20ISPS%20code.pdf (accessed on 19 June 2015).

- The aspects related to security of non-SOLAS ships operations.
- The basic provisions for receipt of Ship Security Assessment.[214]
- Training of duly authorized officers.
- Pre-arrival information requirements for ships.[215]

4.6 *The progress made by the ISPS Code in fulfilling its purpose*

The foremost objective of the ISPS Code is to address security concerns in maritime transportation, specifically, terrorism. However, its provisions also addresses other security issues such as theft, piracy and smuggling which is an additional benefit of the ISPS Code.

IMO Safety Division authors, Hesse and Charalambous indicate that the organisation views the enhanced security measures in a positive light. These authors note that the new security measures provide not only protection from terrorist and other criminal acts but also enhance the efficiency of the maritime industry by the:

- Reduction in delays
- Quicker handling times
- Improved asset control
- Reduced losses owing to theft
- Decrease in the cost of insurance[216]

4.7 *Recommendations to the IMO*

In light of the inadequacies and inconsistencies identified in the ISPS Code, the following recommendations were made to IMO by Hesse in order to address the situation:

- Model national legislations and guidelines should be developed with specific focus on the implementation process.
- Security-related operation of non-SOLAS vessels should be provided guidance.
- Provide direction on the basic and specific security-related training.
- Provide guidance on conduct of exercises and drills that is security-related.
- To conduct regional workshops and seminars on a periodical basis.[217]

[214]Ibid.
[215]Ibid.
[216]H Hesse and N L Charalambous op cit n 37 at 135.
[217]Ibid.

Additional recommendations for the IMO:

- Strong collaboration and coordination at international and national levels regarding systems and processes for improving the ISPS Code.
- Assistance and direction to vessels that find them themselves in difficulties after calling at a high-risk port. [218]
- The ISPS Code should be amended in order to include the various maritime security threats including piracy.[219]
- Amendment of the ISPS Code to address its enforceability by specifically amending the IMO Member State audit scheme to become mandatory instead of voluntary.[220]
- The development of a global maritime security network as cooperation between nations can address the concerns of this international threat.[221]
- To increase the effectiveness of the implementation of the ISPS Code, Contracting Governments should include in its national legislation of the ISPS Code, emergency plans and response systems in order to address real attacks and or security incidents.[222]
- Development of a Regulation that would enhance the maritime security of ships that fall outside the scope of the ISPS Code. In doing so it would close the loophole in the provisions and protect itself against possible exploitation by criminal networks.

4.8 *Conclusion*

Maritime security threats in a number of Contracting States have been effectively addressed by the implementation of the ISPS Code. The maritime environment can strengthen the effectiveness and enforceability of the ISPS Code through the implementation of recommendations made by various authorities and learned persons in the maritime field.

Identifying inadequacies, inconsistencies and also realising the true potential of the ISPS Code is essential for the success of this relatively new piece of legislation. Finding solutions to challenges experienced in the implementation of the ISPS Code is part of the process

[218]L H Bergqvist op cit n 113.
[219]Ibid.
[220] J Jibkwon op cit n 16 at 74.
[221]LCDR Jon D. Peppetti, JAGC, USN 'Building a Global Maritime Security Network" (2008) 55 *Naval Law Review* 73.
[222] J Jibkwon op cit n 16 at 72.

refining the ISPS Code as well as enhancing its effect and efficiency and as such the opinions of various participants in the maritime industry should be considered.

The IMO playing such a prominent role in maritime security in consistently reviewing its legislation in order to improve its value to the maritime community and such introducing methods and programmes to ensure that gaps identified is closed. For instance IMO has acknowledged that its inability to enforce its Regulations as that is the responsibility of the Contracting Governments, the IMO can only monitor compliance.[223] However the IMO addresses this situation by introducing "train-the-trainer" programme which is aimed at providing assistance of the implementation process of the ISPS Code. Those that are responsible for training and implementation of the ISPS Code will be trained by Instructors of the IMO who are qualified and approved.[224]

Furthermore, gaps/challenges/weaknesses/shortcomings experienced and identified regarding the application of the ISPS Code should be relayed to the IMO as well as Contracting Governments in order to improve maritime security.

South Africa has acted on its responsibility as one of the SOLAS Member states by implementing the ISPS Code via its domestic legislation, namely The Merchant Shipping (Maritime Security) Regulation 2004, which is a comprehensive and concise guide on how to enhance its maritime security measures. In addition, South Africa's commitment of ensuring that its maritime environment is secure is demonstrated in the adoption of Regulation 2004 and more importantly through the compliance of all eight of its commercial ports to the regulation.

[223] F McNaught op cit n 111.
[224] CZ Raymond op cit 193 at 3.

BIBLIOGRAPHY

Primary Sources

Conventions

1. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA).
2. International Convention for the Safety the Life at Sea (1974), as amended.

Legislations

1. The Constitution of South Africa Act 108 of 1996.
2. The National Ports Act 12 of 2005.
3. The Merchant Shipping (Maritime Security) Regulations, 2004.
4. Draft South African Maritime Transport Policy (2008).
5. SAMSA Act 5 of 1998.
6. International Ship and Port Security Code, Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended.
7. 1988 Rome Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA).
8. 1988 Rome Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf.
9. United States Maritime Transport Security Act of 2002.
10. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on Enhancing Ship and Port Facility Security.

Maritime Notices/Circulars

1. ISPS Vessel Clearance Procedure, Policy Number: SMP 3/2010.
2. SAMSA Marine Notice 12 of 2008.
3. SAMSA Marine Notice No. 20 of 2014.
4. SAMSA Marine Notice 33 of 2014.
5. SAMSA Marine Notice 5 of 2015.
6. MSC/Circ. 1074.
7. MSC/Circ. 443.
8. MSC.1/Circ.1283
9. (MSC)/Cir 1154.

Secondary Sources

Journals Articles & Research Papers

1. Balkin, R 'The International Maritime Organisation and Maritime Security' (2006) 30 Tulane Maritime Law Journal 3.
2. Barnett D 'Al-Furqan Brigades claims two attacks on ships in Suez Canal, threaten more' (2013) A blog of the long war Journal.
3. Bateman S. 'Assessing the Threat of Maritime Terrorism: Issues for the Asia-Pacific Region' (2006) 12(3) 81.
4. Bezkorovainiy V. and Sokolyuk S. 'Piracy, Maritime Terrorism and Disorder at Sea' (2012) Corbett Paper No 8 at The Corbett Centre for Maritime Studies.
5. Bergqvist L.H. 'The ISPS Code and Maritime Terrorism' (2014).
6. Bryant D L 'Historical and Legal Aspects of Maritime Security' 17 U.S.F Maritime Law Journal.
7. Burmester C. 'International Ship and Port Facility Security (ISPS) Code – Perceptions and Reality of Shore based and sea-going staff' (2004) Southampton Institute of Higher Education, United Kingdom.
8. Coelho JPB. 'African Approaches to Maritime Security: Southern Africa' (2013) FES Peace and Security.
9. Forrest C. 'The Balancing of Maritime Interests in the Southern African Oceans in Light of the New International Maritime Security Regime' (2008) 41 (1) The Comparative and International Law Journal of Southern Africa.
10. Hesse H. and Charalambous N.L. 'New Security Measures for the International Shipping Community' (2004) 3 (2) WMU Journal of Maritime Affairs 123–138.
11. Hesse HG '3 years on –What are the Global Issues in Maritime Security' (2007).
12. Jibkwon J. 'Progress and Challenges: Ten years after the ISPS Code' (2013) World Maritime University, Sweden 20.
13. Joubert L. World Maritime University 'The extent of maritime terrorism and piracy: a comparative analysis' (2013) Journal of Military Studies Vol 41, No 1 pp111-137.
14. Joyner C. 'Navigating Troubled Waters: Somalia, Piracy, and Maritime Terrorism' (2009) 10 (2) Georgetown Journal of International Affairs 83.
15. LCDR Jon D. Peppetti, JAGC, USN 'Building a Global Maritime Security Network" (2008) 55 Naval Law Review 73.
16. Lloyd's Register Marine 'ISPS Code'.

17. Louw-Vaudran L. ‘What does ensuring SADC's maritime security mean for South Africa?’ (2014).
18. Karigithu N. ‘Port Security: The ISPS Code’ (2008) available at www.pmaesa.org/media/.../Kenya_Maritime_Authority_Djibouti_2008.
19. Maharaj Dr A. ‘Economic Development Position Paper on Port Expansion’ (2013).
20. McNaught F. ‘Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the Maritime Security Threat’ (2005) Geddes Paper 91.
21. Minnaar A. ‘Border Control and Regionalism: The Case of South Africa’ (2001) 10 (2) African Security Review.
22. Nelson E.S. ‘Maritime Terrorism and Piracy: Existing and Potential Threats’ (2012) 3(1) Global Security Studies 20.
23. Raymond C.Z. ‘Maritime Terrorism in Southeast Asia: Risk Assessment’ (2005) 75 Institute of Defence and Strategic Studies Singapore.
24. Saeedi S.N. , Khodakhshi S. and Jafari H. ‘An Empirical Study on Effects of ISPS Code Implementation on Iran’s Port Activities’ (2012) ISSN 2322-2360 (7).
25. Schoenbaum, T.J. and Langston, J.C. ‘An All Hands Evolution: Port Security in the Wake of September 11t’ (2003) 77 Tulane Law Review 1345.
26. SeaNews Turkey article ‘Fire, explosion aboard 10,061-TEU Cosco Asia in Suez terror attack’ International Shipping Magazine.
27. Siko M. 'South Africa's Maritime Interests and Responsibilities' (1996) 5 African Security Review.
28. Trelawny C. ‘Maritime Security: Implementation of the ISPS Code’ (2005) IMO 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference Dar es Salaam.
29. Turack D.C. ‘Maritime Terrorism and International Law’ (1992) 41 (2) The International and Comparative Law Quarterly 490.
30. United Nations Conference on Trade and Development ‘Maritime Security: ISPS Code Implementation, Costs and related Financing’ (2007) UNCTAD Secretariat.
31. William P. ‘The Implementation of the ISPS Code in New Zealand and Regional Issues for Discussion’ Presented to the government by the Deputy Director Safety and Response Services Maritime Safety Authority.

Port Authorities and Press Releases

1. American Association of Port Authority 'Five Years After 9/11 Attacks: U.S. Ports More Secure Than Ever; Progress must Continue' (2006) available at http://www.aapa-ports.org/Press/PRDetail.cfm?ItemNumber=1092.
2. BBC News 'Guantanamo Prisoner Al-Darbi Admits MV Limburg Attack' (2014) available at http://www.bbc.com/news/world-us-canada-26277556.
3. Bryant D. 'Hijacking of the SS Santa Maria' (2011) Maritime Professional available at http://www.maritimeprofessional.com/blogs/post/hijacking-of-the-ss-santa-maria-13422War II.
4. Gama S, CEO of TNPA presentation "BEE at the National Ports Authority of South Africa" (2004) available at www.transnetnationalportauthority.net.
5. General Assembly Press Release GA/9903, United Nations, Opening its Fifty-Sixth Session, 'General Assembly Condemns Heinous Acts of Terrorism Perpetuated in Host City and Washington' (2001), available at http://www.un.org/News/Press/docs/2001/ga9903.doc.htm.
6. IMO Press Release available at www.imo.org.
    - 'IMO Adopts Comprehensive Maritime Security Measures' (2002)
    - 'ISPS Code and Maritime Security'
    - 'Enhancing Maritime Security'
    - 'Maritime Security Measures Take Shape at IMO' (2002)
    - 'Maritime Security and Piracy'
7. IT Industry News, 'Africa's ports vital for world trade' (2015) available at www.itonline.co.za
8. Nuclear free New Zealand available at http://www.nzhistory.net.nz/politics/nuclear-free-new-zealand/rainbow-warrior.
9. Oman 'Al-Qaeda link confirmed for M Star VLCC Attack' (2010) from Sea trade Maritime News available at www.seatrade-maritime.com/news/asia/al-Qaeda-link-confirmed-for-M-Star-VLCC-attack.html.
10. Port of Belledune, Canada 'Port Security' available at http://www.portofbelledune.ca/security.php.
11. Terrorism Watch and Warning, 'Superferry 14 Fire leaves 116 dead' (2014) available at www.terrorism.com/2014/04/23/superferry-14-fires-leaves-116-dead/.
12. Maritime Port Authority of Singapore 'Port Security: ISPS Code' available at www.mpa.gov.sg.

13. The bombing of Rainbow Warrior available at http://www.greenpeace.org/international/en/about/history/the-bombing-of-the-rainbow-war/.
14. TNPA Compliance Control Plan for the Maritime Security Regulations (2013).
15. Transnet National Port Authority 'A World Class Port Security Service' (2007) available at http://www.transnetnationalportsauthority.net.
16. Transnet National Ports Authority Presentation "Status report on port security in South Africa" (2009) available at www.pmaesa.org/download.php?f=Maritime_ISPS_Status...ppt.
17. UK Department of Transport 'Security Training Requirements in UK Ports for Staff and Approved Training Providers' 2012 available at https://www.gov.uk/guidance/security-training-for-staff-working-in-ports.
18. UK Maritime and Coastguard Agency 'Maritime Safety and Working Conditions' 2012 available at https://www.gov.uk/guidance/maritime-security.
19. Van der Merwe 'ISPS Code- Maritime Security' (2003) available at http://ports.co.za/legalnews/article_2003_08_15_1144.html.
20. Watson K.J. 'Promoting the Creation of an integrated Maritime Security Capability on the Southern African Coast' (2011) Conference.

Thesis

1. Pohlit C 'New Developments in Maritime Security and the Impact on International Shipping' Dissertation submitted at University of Cape Town available at http://uctscholar.uct.ac.za/PDF/1373_Pohlit.pdf .
2. Mazaheri A. 'How ISPS Code affects Ports and Port Activities' (2008), a Thesis submitted to the University College of Boras in Sweden available at www.bada.hb.se/bitstream/2320/3579/1/Ashram%20Mazaheri.pdf.
3. Gunasekaran P 'Port Security in a developing country pre and post 9/11 terrorist attacks: A Case Study on Port Klang in Malaysia' (2012), a Thesis submitted to the University of Greenwich, London.
4. Hellberg P 'Effects of the ISPS Code on Ship and Port Security – A Swedish Perspective' (2009), a Thesis submitted to the World Maritime University in Sweden.

TRANSNET NATIONAL

PORTS AUTHORITY

ISPS VESSEL CLEARANCE PROCEDURE

Policy Number	SMP 3/2010
Version Number	1
Recommended By	Head of Security
Signature	21 January 2011
Supported By	Executive Ports & Corporate Affairs
Signature	25 JANUARY 2011
Supported By	Executive Strategy & Transformation
Signature & Date	
Approved By F. C. PITHEKA	Executive Legal, Risk & Compliance
Signature	

1. PREAMBLE

Transnet National Ports Authority (hereinafter referred to as the "Authority") is, in terms of section 3 (1) of the National Ports Act, 2005 (Act No. 12 of 2005) a port authority which owns, manages, controls and administers all ports of the Republic to ensure their efficient and economic functioning.

2. DEFINITIONS

"a port" means any of the ports defined as such in the National Ports Act, 2005 (Act No. 12 of 2005)

"ISPS Code" – means the International Ship and Port Facility Security Code (as amended from time to time) as mentioned in Chapter X1-2 of the SOLAS Convention;

"SOLAS Convention" – means the International Convention for Safety of Life at Sea, done at London on 1 November 1974, as amended from time to time.

"Regulations"- mean the Merchant Shipping Maritime Security) Regulations, 2004;

"MRCC"- means the maritime rescue co-ordination centre designated under section 11 of the South African Maritime and Aeronautical Search and Rescue Act, 2002 (Act No. 44 of 2002);

"MSCC"- means the Maritime Security Co-ordination Center established by the Director General of the Department of Transport in terms of Regulation 132 of the Regulations;

"maritime transport security incident" - has the meaning given by regulation 103

"maritime security level" means —

(a) maritime security level 1;

(b) maritime security level 2;

(c) maritime security level 3;

"maritime security level 1" means the maritime security level in force in terms of regulation 16 of the Regulations;

"maritime security level 2" means the maritime security level in force under regulation 17 of the Regulations;

"maritime security level 3" means the maritime security level in force under regulation 17 of the Regulations;

"PSO" – means a port security officer appointed as such by the Authority for each of the ports falling under its jurisdiction;

"pre-arrival information" - has the meaning given by regulation 86(3) of the Regulations;

"ship/port interface"- means the interaction that occurs when a security regulated vessel is directly and immediately affected by activities involving —
(a) the movement of persons or goods; or

(b) the provision of port services to or from the ship;

"organ of state" - has the same meaning as in section 239 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996);

"security regulated vessel" has the meaning given by regulation

"ship to ship activity"- means any activity, not related to a security regulated port, that involves the transfer of goods or persons from one ship to another;

"the Act" – means the National Ports Act, 2005 (Act No. 12 of 2005);

3. OBJECTS OF THIS PROCEDURE

To ensure that all the ports falling within the jusrisdiction of the Authority adhere to the same procedures when dealing with maritime security regulated vessels intending to call in any of these ports.

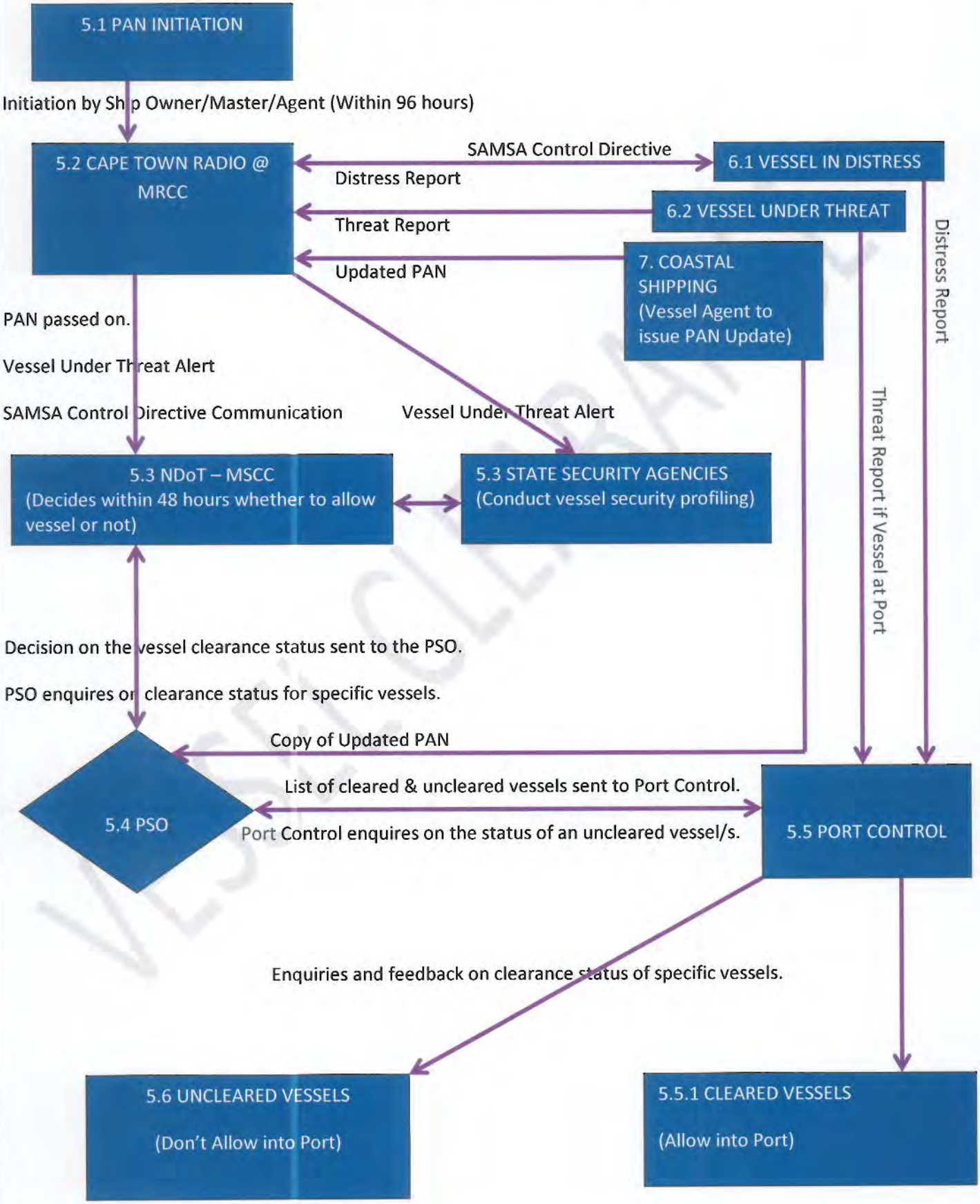
4. APPLICATION

4.1 This Vessel Clearance Procedure applies to the following –

4.1.1 A port owned, controlled, managed and administered by the Authority as defined in the Act; and security regulated vessel as defined in regulations ten (10) and eleven (11) of the Regulations;

4.1.2 This Vessel Clearance Procedure does not however apply to a vessel defined in regulation 4 of the Regulations.

5. PRE – ARRIVAL NOTIFICATION (PAN) PROCESS FLOW



5.1 **PAN INITIATION**

5.1.1 In terms of rule 17 of the Port Rules, at least 96 hours before the arrival in a port of a foreign regulated vessel, the owner, master or agent of that vessel must send to the Authority a copy of the vessel's pre-arrival information that was sent to the South African authorities in terms of regulation 86 of the Regulations;

5.1.2 The South African authorities referred to above is the Cape Town Radio at MRCC;

5.1.3 From the time the pre-arrival information is received by Port Control and the time when the necessary clearance has been received from MSCC by the PSO, no vessel may be allowed to enter a port unless special circumstances dictate otherwise.

5.2 CAPE TOWN RADIO AT MRCC

5.2.1 Once the MRCC has received a pre-arrival notification from the owner/master or agent of a foreign regulated vessel it immediately passes on such request to NDoT – MSCC for further action.

5.3 NDoT – MSCC

In terms of MSCC's practice, it must, within 48 hours from the time the owner, master or agent of the vessel had submited the pre-arrival information to the Cape Town Radio, make a decision regarding whether –

5.3.1 It clears the relevant vessel to enter a port it applied for; or

5.3.2 It is still working on the clearance of the vessel; or

5.3.3 It declines to issue a clearance to the vessel.

The MSCC's decision is then communicated to the PSO of the relevant port.

5.4 PORT SECURITY OFFICER (PSO)

On receipt of the Vessel Clearance List (VCL), the PSO –

5.4.1 Must, by e-mail, or what ever eletronic means inform Port Control at least thirty-six (36) hours before the expected arrival of cleared vessels in that port. Such information must be relayed at least two times in a day;

5.4.2 Only information relevant to that port must be communicated to Port Control;

5.4.3 Where a vessel has been cleared to enter a port, the PSO must notify the relevant vessel agent accordingly. This notification must include the Vessel Information in its entirety (all fields); and

5.4.4 Where VCL reflects "awaiting Pre-arrival Notification" in respect of a particular vessel, the PSO must, in writing, advise the relevant vessel agent to re-submit the Pre-arrival Notification;

5.4.5 Where the VCL indicates a change in vessel security level status from the time when the vessel submitted its Pre-arrival Information, the PSO must immediately, and in writing, notify the vessel agent of such a change in security status; and the relevant PFSO;

5.4.6 Keeps records of Vessel Clearance Lists, both as a hard copy as well as soft copies.

5.5 **PORT CONTROL**

Port Control must –

5.5.1 Not permit a vessel to enter a port unless such vessel has been ISPS cleared by MSCC to do so;

5.5.2 Not engage vessel agents regarding maritime security related matters;

5.5.3 Notify the PSO of vessel/s calling to a port without the necessary MSCC security clearance;

5.5.4 Provide, where required, the PSO with information relating to the itinerary of a particular vessel (supply eletronically with short analysis of data);

5.5.5 Immediately advice the PSO about any ship to ship interface inclusive of any unathorised aircraft interfacing with any vessel at outer anchorage;

5.5.6 Ensure vessels not cleared by MSCC remain outside outer anchorage;

5.5.7 Timeously notify the PSO of any vessel in need of assistance which needs access to a port even prior to clearance has been received from MSCC;

5.5.8 Ensure proper records are kept of vessels engaged in coastal shipping, as and when such information is received from the PSO of that port.

5.6 **VESSELS NOT CLEARED BY MSCC**

Such a vessel/s must –

5.6.1 Remain clear of outer anchorage and outside the approaches to a port;

5.6.2 Not be approached by any craft (including aircraft) except law enforcement or TNPA craft;

5.6.3 Not have a surveyor or any other service delivered to it without the permission of the Authority;

5.6.4 Not interface with any other vessel.

6. OTHER VESSELS THAT MAY ENTER THE PORT ON SPECIAL ARRANGEMENTS

6.1 **VESSEL IN NEED OF ASSISTANCE (VESSEL IN DISTRESS)**

6.1.1 The vessel in need of assistance must first report the emergency to the Cape Town Radio (MRCC) where SAMSA will issue a control direction to the ship; and also report to the relevant Port Control;

6.1.2 When making such a report to Port Control, the vessel must furnish the Authority with a brief statement relating to the emergency;

6.1.3 It may be necessary that Law Enforcement officers may be required to board vessel to confirm emergency;

6.1.4 The Port Control must immediately advise the PSO of the request.

6.1.5 The PSO must –

6.1.5.1 Confirm with MRCC whether a request has been received by them from the affected vessel;

6.1.5.2 Continuously liaise with the Harbour Master in charge;

6.1.5.3 Within eight (8) hours from the time the PSO has received information about the vessel in need of assistance, it must furnish the MSCC with a comprehensive statement regarding the vessel. Such statement must also include safety of the crew and the vessel itself;

6.1.6 Only when the Authority is satisfied that the request is authentic and that the port integrity or its security will not adversely be compromised, may the Harbour Master allow a vessel into a port.

6.2 **VESSEL UNDER THREAT**

6.2.1 A vessel under threat in the territorial waters of the Republic must communicate with the MRCC, who will forward the alert to the appropriate authorities;

6.2.2 A vessel under threat at a South African port can communicate with the local Port Control, who should then notify PSO, SAPS, or anybody else required as per the list of key role players;

6.2.3 The Security Level at a particular Facility or the entire Port shall be increased where necessary after consultation with all responsible State Security Agencies as well as the Director General at the National Department of Transport.

7. **COASTAL SHIPPING**

The vessel agent must –

7.1 Supply an updated PAN to MRCC;

7.2 Forward a copy of this updated PAN to the PSO and also give the original GI number that vessel submitted for orginal clearance which lists (the date and the Port the vessel was orginally cleared in). Agent must also confirm in writing whether the vessel, en route to the next port in the Republic has-

7.2.1 Left South African waters;

7.2.2 Interfaced with a non ISPS vessel; or;

7.2.3 Had a reportable Maritime Incident on board the vessel.

7.3 The PSO must verify whether the vessel was cleared in the mentioned port, by referring to the first clearence list, and where practicable, the PSO must request access to the VTS log and indicate in remarks column;

7.4 If he or she is satisfied, the PSO must forward a copy of the pre-arrival notification (PAN), and the Line from the orginal Clearence Lists to Port Control.

8. **MARITIME SECURITY INCIDENT IN A PORT AND OUTER PORT LIMITS (OPL)**

Where a maritime security incident in a port occurs –

8.1 The vessel must immediately inform Port Control of the incident having occurred;

8.2 Port Control must immediately thereafter inform the PSO by e-mail or any agreed/standard communication channels;

8.3 Once the PSO has received the information, he or she must advise the relevant security agencies which include SAPS, SSA, DHA and SARS;

8.4 The PSO has a duty to, as urgently as practicably possible, advise the MSCC and the Transnet National Port Authority's National Head of Security of the nature of the incident and possible threat/risk to the port.

South African
Maritime Safety Authority

Marine Notice No. 12 of 2008

The Merchant Shipping (Maritime Security) Regulations, 2004

TO MASTERS AND OPERATORS OF INTERNATIONALLY TRADING SHIPS BOUND FOR SOUTH AFRICAN PORTS, THEIR AGENTS, SOUTH AFRICAN ASSOCIATION OF SHIP OPERATORS AND AGENTS, HARBOUR MASTERS, CAPE TOWN RADIO, THE MARITIME RESCUE CO-ORDINATION CENTRE (MRCC) AND OTHER INTERESTED PARTIES

Marine Notices Nos. 20 of 2004 and 33 of 2005 are cancelled

Summary

This marine notice gives guidance to the industry on the application of the *Merchant Shipping (Maritime Security) Regulations, 2004*, and the International Ship and Port Facility Security (ISPS) Code.

1 South Africa has implemented the Maritime Security requirements contained in Chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974, and the International Ship and Port Facility Security (ISPS) Code through the *Merchant Shipping (Maritime Security) Regulations, 2004*. These regulations apply to South Africa's seven major ports, namely Saldanha Bay, Cape Town, Mossel Bay, Port Elizabeth, East London, Durban, and Richards Bay. They also apply to passenger ships, cargo ships of 500 or more gross tonnage and mobile offshore drilling units (MODUs) on international voyages. However, they do not apply to fishing vessels, vessels used solely for sport or recreation, government ships engaged solely on non-commercial voyages, coasting ships, and ships transiting South Africa's territorial waters.

Certification of South African ships

2 The South African Maritime Safety Authority (SAMSA) is responsible for approving ship security plans for South African ships, for verifying compliance with plans, and for issuing the International Ship Security Certificate (ISSC) and Continuous Synopsis Record (CSR).

Security Level in South African territorial waters

3 Security Level 1 applies in South Africa's territorial waters. Any change of security level or its area of application will be notified by Marine Notice, Navigational Warning and Notices to Mariners.

Port security

4 Security Level 1 is the default security level applying to South Africa's seven major ports (and the port facilities in these ports). Any change of security level will be declared by the Director-General: Transport, who is required to give proper notice of the declaration.

5 In accordance with Regulation XI-2/9 of the International Convention for the Safety of Life at Sea, 1974, and paragraph B/4.39 of the International Ship and Port Facility Security (ISPS) Code the Director-General: Transport has under the *Merchant Shipping (Maritime Security) Regulations, 2004*, determined the requirements for ***pre-arrival*** and ***pre-entry information***. The full official text of the determination is published by Government Notice No. R. 1412 in Government Gazette No. 27048 of 10 December 2004.

6 Pre-arrival information is required from foreign passenger ships, cargo ships of 500 or more gross tonnage and mobile offshore drilling units (MODUs) on international voyages bound for South African ports.

7 These requirements do not apply to fishing vessels, vessels used solely for sport or recreation, government ships engaged solely on non-commercial voyages, coasting ships, and ships transiting South Africa's territorial waters, including ships calling off-limits at a South African port for the transfer of stores, crew, landing an ill crew member, etc. However, for ships calling off-limits voluntary compliance is encouraged and may avoid delay in the event, for example, of transfer operations having to be done within port limits because of adverse weather conditions.

8 Reports are not required from ships making voyages between South African ports (i.e. coasting). If a ship makes a voyage to a port in another country (e.g. Maputo - Mozambique or Walvis Bay - Namibia), a pre-arrival/pre-entry information report must be made before any subsequent call at a South African port. Also, when a ship is coasting between South African ports and interfaces with another ship between ports, the master must transmit a pre-arrival/pre-entry information report as soon as possible, but at least 5 hours before the ship's ETA.

9 The **format and content of the pre-arrival/pre-entry information report is given in Annex A.** Masters are advised to exercise care when drafting reports, particularly when using a single / or double //. The report comprises groups of words and numbers identified by a prefix, with a double // used to separate the groups and a single / used to separate words or numbers within a group. It should be noted that in the format of the report field “B” is the time of making the report and field “J” is the ETA at the first port of call. There should be at least a 96 hours difference in the times.

10 **The report must be made at least 96 hours before the ship’s expected time of arrival (ETA) at the first South African port.** If the ship is arriving from a foreign port where the voyage time between ports is less than 96 hours, the master must ensure that the pre-arrival/pre-entry information is sent in compliance with the 96 hour requirement and updated when the ship clears the last foreign port.

11 An amended report must be made if:

.1 the ETA date for the ship changes; however, a change in time on the same day need not be reported; or

.2 there has been a ship-to-ship or ship/port interface after the original report was made; or

.3 any other information in the original report changes, excluding those noted in 11.1.

12 The Maritime Rescue Coordination Centre (MRCC) in Cape Town is the second point of contact for pre-arrival/pre-entry information. **The pre-arrival/pre-entry information report must be in English and in writing, and is to be transmitted to the MRCC via Cape Town Radio, (the first point of contact)**. The MRCC will only accept reports directly from the ship via Cape Town Radio; no reports by voice communication will be accepted. The role of the MRCC is to scrutinise reports for correctness and completeness.

13 The MRCC does not security-clear ships. Its function is to check pre-arrival/pre-entry information reports to ensure relevance and completeness. If MRCC has any queries regarding the

ship's report, it will communicate with the ship via Cape Town Radio. The MRCC forwards checked reports to the Maritime Security Co-ordination Centre (MSCC), which is responsible for informing port security officers (PSO) about ships' security clearance status. **Ships' agents should, therefore, obtain security clearance information from the relevant PSO directly**.

14 The preferred means of ship-to-shore communication for pre-arrival/pre-entry information reports is via telex. The telex system assures receipt of the message at Cape Town Radio. **The report can be transmitted on telex number 095 511600 or alternatively on 095 521846**. (The prefix 095 is the international dialing code). If Inmarsat C is used, the ship's officer can confirm receipt by selecting the option "request delivery confirmation" on the ship's terminal. A ship's agent can also confirm receipt 6 hours after transmission by contacting Cape Town Radio on the help line 0800 222 208.

15 Transmission by means other than telex has resulted in communication difficulties which, in turn, have caused delays to ships. Only in exceptional cases such as faulty or unavailable satellite communication, will Cape Town Radio accept a forwarded e-mail message from a ship's agent (provided the agent confirms receipt of the e-mail with Cape Town Radio). Cape Town Radio will not forward an e-mail message to the MRCC without this confirmation. When e-mail is used, **reports must not be sent as e-mail attachments**, but must be in the e-mail body text because the Cape Town Radio IT system strips attachments from e-mails. Cape Town Radio's e-mail address is maritimeradio@ixmail.co.za

16 Pre-arrival/pre-entry information required by this notice for maritime security purposes is similar to port entry information required by the National Ports Authority (NPA) for berth planning purposes. However, the format and use of this information differs considerably. Masters and agents are advised to ensure that information for the MRCC is not confused with that required by the NPA.

17 **Masters are cautioned that failure to timeously transmit complete and correctly formatted pre-arrival/pre-entry information may result in delays and, in appropriate cases, denial of port entry. Ships whose masters refuse to give pre-arrival/pre-entry information will be denied port entry**.

18 The following table provides information about port security officers (PSOs) at the seven major ports. The contact number in **bold print** in the table is the 24-hour contact number for the PSO.

Port	Name	Telephone	Facsimile	Mobile
Saldanha Bay	Mr S Gaika	**(022) 703 5478**	(022) 703 5484	083 285 3505
Cape Town	Mr T Gagavu	**(021) 449 4270**	(021) 449 2274	083 376 8826
Mossel Bay	Ms D Joyce	**(044) 604 6273**	0866 487 739	072 708 4378
Port Elizabeth	Mr M Mwelase	**(041) 507 1773**	(041) 507 1963/56	083 652 4705
East London	Ms N Sinxoto	**(043) 700 2060/2313**	(043) 700 2070	083 417 3920
Durban	Mr H Strydom	**(031) 361 3771**	(031) 361 8393	083 387 1491
Richard's Bay	Mr W Ndlanzi	**(035) 905 3146**	(035) 905 3126	083 286 2094
The international dialling code prefix for South Africa is +27. The local area code prefix is shown in brackets in the table above. When dialling from outside South Africa, dispense with the 0 in the local code prefix.				

Information regarding port facility security officers (PFSOs) can be obtained from the PSO, the port facility operator or the local ship's agent.

19 The MRCC is also the contact point for ships seeking information on maritime security (excluding confirmation of receipt of the ISPS report) within South Africa's territorial waters. A ship under threat in the territorial waters can communicate with the MRCC, who will forward the alert to the appropriate authorities. The MRCC's Duty Officer can be contacted via Cape Town Radio or as follows:

Telephone : +27 (021) 938 3300
Facsimile : +27 (021) 938 3309
E-mail : mrcc.ct@samsa.org.za

20 A ship under threat at a South African port can communicate with the local Port Control, the PSO, PFSO or the MRCC.

21 A ship security alert signal from a foreign flagged ship will go to the ship owner or flag State and will only be received by the MRCC if the flag State or owner forwards the alert to the MRCC.

SAFREP

22 In the interests of safety all ships are encouraged to participate in the South African Ship Reporting System (SAFREP). This system assists in search and rescue by providing up-to-date information on shipping in the event of a maritime casualty. It is modelled on IMO Resolution A.851(20) regarding general principles for ship reporting requirements. It makes use of movement reports submitted to Cape Town Radio by ships within the South African search and rescue region. Participation in the system is voluntary. Information regarding SAFREP may be found in the Admiralty List of Radio Signals.

Anchoring outside port limits

23 Masters, owners and operators are reminded that it is an offence in terms of the Marine Traffic Act, 1981, to anchor or stop a ship (for repairs or otherwise) in South Africa's territorial or internal waters outside port limits without permission from SAMSA. Permission to anchor or stop may be obtained by submitting to the MRCC a pre-arrival information report together with a request to anchor or stop. The MRCC will forward the request to the local Principal Officer for decision.

24 A ship that has to anchor or stop in an emergency must inform SAMSA as soon as possible, but at least within one hour after anchoring or stopping. Masters are reminded that SAMSA has the authority, even in an emergency, to set conditions for anchoring or stopping.

12 August 2014

SM6/5/2/1
SM7/3/2/1/2

Issued by and obtainable from:
The South African Maritime Safety Authority
161 Lynnwood Road
Brooklyn, Pretoria

PO Box 13186
Hatfield 0028

Tel: +27 12 366 2600
Fax:+27 12 366 2601
E-mail: marinenotices@samsa.org.za
Web Site : www.samsa.org.za

ANNEX

FORMAT AND CONTENT OF PRE-ARRIVAL/PRE-ENTRY INFORMATION REPORT

Code prefix	Content	Explanation
A	Ship name/Call sign/Port of registry/Current security level on board	Ship name, call sign, port of registry of the ship, current security level e.g. /SHIPNAME/ABCD/MONROVIA/1//
B	Time	Time of report in UTC. 6 digit date time group giving day of the month and hours and minutes in UTC followed by the month e.g. /291000 SEP//
C	Position	The position of the ship at the time of reporting. 4 digit group giving latitude in degrees and minutes suffixed with "N" (north) or "S" (south) and 5 digit group giving longitude in degrees and minutes suffixed with "E" (east) or "W" (west) e.g. /1212S 00527W//
D	Ship type	Type of ship written in full e.g. /CONTAINER VESSEL//
E	Course	3 digit group for the present true course being steered e.g. /052//
F	Speed	The ship's speed in knots with the decimal omitted e.g. 16.8 knots = /168// or 8.7 knots = /087//
G	IMO number	IMO ship identification number e.g. /IMO1234567//
H	ISSC confirmation on board/Issuing authority	Confirmation yes or no (Y/N) and issuing authority e.g. /Y/LIBERIA//
I	Business name of ship's agent at intended first SA port of call	Shipping agent company name e.g. /STURROCKS//
J	First SA port of call and ETA and all subsequent SA ports of call with ETAs and first port of call after SA	Name of first SA port of call with ETA as per (B) above and all subsequent SA ports of call in voyage order until departure from SA waters with ETAs and first port of call after SA e.g. /DURBAN – 291000/PORT ELIZABETH – 301900/CAPE TOWN – 010500/SINGAPORE//
P1	Last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /MUMBAI – INDIA/01062004/1/NIL/Y//
P2	Second last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Second last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /PORT LOUIS – MAURITIUS/28052004/1/NIL/Y//
P3	Third last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Third last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /MOMBASA – KENYA/20052004/2/APPOINTED SECURITY COMPANY/Y//
P4	Fourth last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Fourth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /DAR ES SALAAM – TANZANIA/14052004/1/NIL/Y//

Code prefix	Content	Explanation
P5	Fifth last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Fifth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /MOMBASA – KENYA/10052004/1/NIL/Y//
P6	Sixth last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Sixth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /NACALA – MOZAMBIQUE/02052004/1/NIL/Y//
P7	Seventh last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Seventh last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /BEIRA – MOZAMBIQUE/10042004/1/NIL/Y//
P8	Eight last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Eighth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /MAPUTO – MOZAMBIQUE/06042004/1/NIL/Y//
P9	Ninth last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Ninth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /LUANDA – ANGOLA/30032004/1/NIL/Y//
P10	Tenth last port of call/Departure date/Ship security level/Security measures and procedures/Ship to ship measures	Tenth last port and country of call/Departure date in 8 digit group (DDMMYYYY)/Security level/Any special or additional security measures taken by ship during the ship-port interface/That the appropriate security procedures were maintained during ship to ship activity in this port (Y/N) e.g. /WALVIS BAY – NAMIBIA/24032004/1/NIL/Y//
Q	Registered owner (or bareboat charterer) and contact details	Name of registered owner (or bareboat charterer)/Contact address/Telephone number/Fax number/E-mail address (if available) e.g. /SA SHIPPING/POBOX111CAPE TOWN/+21546783/+21546787/SHIPPING@SHIPPING.NET.ZA//
R	Ship security officer details	Name of ship security officer/Rank of ship security officer e.g. /SMITH/CHOFF//
S	Company security officer details	Name of company security officer/Contact telephone number/Mobile telephone number/E-mail address(if available) e.g. /HOUTON/+215467824/0824352614/JHOUTEN@SHIPPING.NET.ZA/ /
U	Details of cargo	General description of cargo on board and hazardous cargo as per IMDG Code e.g. /72CARS/624 CONTAINERS WITH GENERAL/2 CONTAINERS CLASS 4.1/ 6 CONTAINERS CLASS 2.2/1 CONTAINER CLASS1.1//
W1 – W(x)	Details of crew members	Information about persons on board designated as crew showing surname, name, gender, birth date (DDMMYYY), nationality, travel document number, document expiry date e.g. /SOAP, JOE, MALE, 01121954, BRITISH, C2361, 23012007//

Code prefix	Content	Explanation
X1 – X(x)	Details of passengers	Information about persons on board designated as passengers showing surname, name, gender, birth date (DDMMYYY), nationality, travel document number, document expiry date e.g. /SWART, HANS, MALE, 07041970, SOUTH AFRICAN, C78965, 15052005//
Y1 – Y(x)	Details of persons on board, other than passengers or crew, with the reason for being on board	Information about persons on board who are not passengers or crew showing surname, name, birth date (DDMMYYY), nationality, travel document number, and reason for being on board (if available) e.g. /BLOGGS, HENRY, 06111949, SOUTH AFRICAN, C12345, SURVIVOR//

SAMPLE PRE-ARRIVAL/PRE-ENTRY INFORMATION REPORT

A/SHIPNAME/ABCD/MONROVIA/1//
B/291000 SEP//
C/1212S 00527W//
D/CONTAINER VESSEL//
E/052//
F/168//
G/IMO1234567//
H/Y/LIBERIA//
I/STURROCKS//
J/DURBAN – 291000/PORT ELIZABETH – 301900/CAPE TOWN – 010500/SINGAPORE//
P1/MUMBAI – INDIA/01062004/1/NIL/Y//
P2/PORT LOUIS – MAURITIUS/28052004/1/NIL/Y//
P3/MOMBASA – KENYA/20052004/2/APPOINTED SECURITY COMPANY/Y//
P4/DAR ES SALAAM – TANZANIA/14052004/1/NIL/Y//
P5/MOMBASA – KENYA/10052004/1/NIL/Y//
P6/NCALA – MOZAMBIQUE/02052004/1/NIL/Y//
P7/BEIRA- MOZAMBIQUE/10042004/1/NIL/Y//
P8/MAPUTO – MOZAMBIQUE/06042004/1/NIL/Y//
P9/LUANDA – ANGOLA/30032004/1/NIL/Y//
P10/WALVIS BAY – NAMIBIA/24032004/1/NIL/Y//
Q/SA SHIPPING/POBOX111CAPE TOWN/+21546783/+21546787/SHIPPING@SHIPPING.NET.ZA//
R/SMITH/CHOFF//
S/HOUTON/+215467824/0824352614/JHOUTEN@SHIPPING.NET.ZA//
U/72CARS/624 CONTAINERS WITH GENERAL/2 CONTAINERS CLASS 4.1/6 CONTAINERS CLASS 2.2/1 CONTAINER CLASS1.1//
W1/SOAP, JOE, MALE, 01121954, BRITISH, C12361, 23012007//
X1/SWART, HANS, MALE, 07041970, SOUTH AFRICAN, C78965, 15052005//
Y1/BLOGGS, HENRY, 06111949, SOUTH AFRICAN, C12345, SURVIVOR//

South African Maritime Safety Authority

Ref: **SM 6/5/2/1**
SM 1/5/1/59/3

Date: 22 August 2014

Marine Notice No. 20 of 2014

MERCHANT SHIPPING (Maritime Security) Regulations, 2004; "Unlawful Interference with Maritime Transport" – STOWAWAYS. SOLAS – CHAPTER XI – 2 Maritime Security.

TO ALL SHIP OWNERS, MASTERS, AGENTS

Summary

This Notice is a general advisory notice to the industry regarding **stowaways** on board ships specifically departing ports along the West African Coast.

This Notice is to advise Masters of ships departing ports along the coast of West Africa to pay special attention, immediately after sailing from the last port, to carry out a thorough inspection of the ship spaces that may be accessed without clearing the ship gangway security. Particular attention is to be directed to the RUDDER TRUNK SPACE.

Vessels departing from ports of the West Coast of the African Continent bound for South Africa find, upon arrival at the first port of call stowaways in the rudder trunk space of the ship.

It is alleged that these people embark the ship when alongside, especially in ports having river access, with the aid of dugout canoe or small rowed boats.

SOLAS Chapter XI-2: Special Measures to Enhance Maritime Security.

Regulation 1. ***Definitions.***

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

Regulation 2. ***Application.***

1. This chapter applies to:

.1 the following types of ship engaged on international voyages:

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

.1.2 cargo ships, including high- speed passenger craft, of 500 gross tonnage and upwards; and

.1.3 mobile offshore drilling units; and

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

Reading from the **International Ship and Port Facility Security Code** (ISPS Code),

Part B, Item 8 (*Ship Security Assessment*).

8.9 The SSA (Ship Security Assessment) should consider all possible threats, which may include the following types of security incident:

.4 unauthorized access or use, including presence of stowaways;

Reading also;

9.9 The SSP (Ship Security Plan) should establish the security measures covering all means of access to the ship identified in the SSA. This should include any (*but is not restricted to*):

.1 access ladders;

.2 access gangways;

.3 access ramps;

.4 access doors, side scuttles, windows and ports;

.5 mooring lines and anchor chains; and

.6 cranes and hoisting gear. ***Adding;***

.7 *access to void spaces in particular* ***the rudder trunking space.***

Quoting from **Part A, Requirement 19.** (*Verification and Certification for Ships.*)

19.1 Verifications.

.1 Each ship to which this Part of the Code applies shall be subject to the verifications specified below:

.1 an initial verification before the ship is put into service or before the certificate required under section 19.2 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 this Part of the Code and of the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and this Part of the Code, is in satisfactory condition and fit for the service for which the ship is intended.

19.2 Issue and Endorsement of Certificate.

.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

Application of this Marine Notice.

The Master of any ship departing the last port of call along the West Coast of the African Continent, specifically bound for South Africa or in fact, for any other next port of call, is to apply whatever facilities are available at that port, enabling the ship's Security Officer to conduct a thorough search of the rudder trunk space having external access to this space via the rudder.

Furthermore, at the earliest opportunity, the owner of the any ship operating along this coastline, is to make arrangements for suitable gratings to be welded over this access position, thereby preventing any external human access into the rudder trunk space.

NOTE: This external human access prevention grating shall not, in any way possible, hinder the full operation of the ship's steering mechanism. The ship's Classification Society's approval of this modification will also be recommended.

In addition and at this present time, failure to eliminate the transportation of STOWAWAYS from this coast line, may pose serious health risks and ship safety concerns.

22 August 2014

SM 6/5/2/1
SM 1/5/1/59/3

Issued by and obtainable from:
The South African Maritime Safety Authority
146 Lunnon Road
Hillcrest, Pretoria

PO Box 13186
Hatfield 0028

Tel: +27 12 366 2600
Fax:+27 12 366 2601
E-mail: marinenotices@samsa.org.za
Web Site : www.samsa.org.za

South African Maritime Safety Authority

Ref: **SM6/5/2/1**
SM12/5/5/3

Date: **30 March 2015**

Marine Notice No. 5 of 2015

Procedures to be followed for Bulk Cargo Shipment which are not listed in the IMSBC Code.

TO SHIP OPERATORS, MASTERS, SHIPS' AGENTS AND PRINCIPAL OFFICERS

Summary

This marine notice lists the procedure to be followed for bulk cargoes which are not listed in the IMSBC Code

It is apparent that a degree of confusion currently exists within the shipping industry as to the statutory procedures which have to be complied with for the shipment of solid bulk cargoes which are not listed in the IMSBC Code.

All parties involved in the shipment of solid bulk cargoes shall ensure that they have available and readily at hand the latest current edition of the IMSBC Code (International Maritime Solid Bulk Cargoes Code) which is published by I.M.O. This publication which is updated at regular intervals lays down in great detail information as to the manner in which solid bulk cargoes should be shipped and should always be consulted prior to planning actioning any shipment. The procedures / actions to be complied with for listed cargoes are laid down within the code.

The procedures to be followed for **unlisted** cargoes are dealt herewith. All concerned should strictly adhere to these procedures which are statutory. Non-compliance and improper planning of shipments will prejudice marine safety and undoubtedly lead to costly delays.

Shipments of unlisted cargoes require SAMSA approval. Provisions of the IMSBC apply to all vessels to which the SOLAS convention as amended applies and are carrying solid bulk cargoes. Application accompanied by the required documentation should be timeously submitted to the Principal Officer SAMSA at the intended port of loading.

The following summarises the procedures for unlisted cargoes. The code should be consulted for detailed advice. **(See section 1, item 1.3 through to item 1.3.3, pages 9 and 10 of the 2013 edition of the code)**

- When a solid bulk cargo that is not listed in appendix 1 of the code is proposed for carriage in bulk, the shipper shall prior to loading provide SAMSA at the port of loading with the characteristics and properties of the cargo in accordance with Section 4 of the code. Based on the information received, the Authority (SAMSA) will assess the acceptability of the cargo for safe shipment.

- Section 4 of the code relates to assessment of acceptability of consignments for safe shipment. (IMSBC Code 2013 Edition, Page 25). Section 4 deals with:-
    1. Identification and classification. (4.1)
    2. Provision of information. (4.2)
    3. Form for cargo information. (4.2.3)
    4. Certificates of test. (4.3)
    5. Sampling procedures. (4.4)
    6. Interval between sampling / testing and loading for TML (Transportable Moisture Limit) and moisture content determination. (4.5)
    7. Sampling procedures for concentrate stockpiles. (4.6)
    8. Examples of standardised sampling procedures, for information. (4.7)
    9. Documentation required on board the ship carrying dangerous goods. (4.8)

- When it is assessed that the solid bulk cargo proposed for shipment may possess hazards as those defined in Group A or B of the code and as defined in 1.7 (Definitions) advice is to be sought from the competent authorities of the port(s) of unloading and the flag state of the carrier.. The three competent authorities will set the preliminary suitable conditions for the carriage of the cargo.

- Reference should be made to MSC.1/Circ. 1454 of 9 July 2013.

- When it is assessed that the solid bulk cargo proposed for carriage presents no specific hazards for transportation, the carriage of the cargo shall be authorised. The competent authority (SAMSA) shall advise the competent authorities of the port(s) of unloading and the flag state of the carrier of such authorisation.

- The competent authority at the port of loading (SAMSA) shall provide to the Master of the vessel a certificate stating the characteristics of the cargo and the required conditions for carriage and handling of the shipment. The Competent Authority shall also submit an application to the organisation within one year from the issue of this certificate to incorporate the solid bulk cargo into Appendix 1 of the code.

It is again stressed that all parties concerned with both listed and unlisted solid bulk cargoes should have readily at hand an up to date copy of the IMSBC Code and that all applications and documentation should be submitted in full and timeously.

30 March 2015

SM6/5/2/1
SM12/5/5/3

Issued by and obtainable from:
The South African Maritime Safety Authority
146 Lunnon Road
Hillcrest, Pretoria

PO Box 13186
Hatfield 0028

Tel: +27 12 366 2600
Fax:+27 12 366 2601
E-mail: marinenotices@samsa.org.za
Web Site : www.samsa.org.za

APPENDIX TO PART A

APPENDIX 1

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

Certificate Number

Issued under the provisions of the

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

Under the authority of the Government of _____
(name of State)

by _____
(persons or organization authorized)

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 chapter XI-2 of the Convention and part A of the ISPS Code;

3 that the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based .....

This Certificate is valid until .....
subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at .....
(place of issue of the Certificate)

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

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

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

Intermediate verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS*

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

---

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

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

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

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

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

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

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

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

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

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

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

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

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

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

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

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

---

* Delete as appropriate.

** In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

APPENDIX 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

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 _____
(name of State)

by _____
(persons or organization authorized)

Name of ship : .....
Distinctive number or letters : .....
Port of registry : .....
Type of ship : .....
Gross tonnage : .....
IMO Number : .....
Name and address of company : .....
Is this a subsequent, consecutive interim certificate? Yes/ No*
If Yes, date of issue of initial interim certificate.....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 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)

* Delete as appropriate

APPENDIX TO PART B

APPENDIX 1

Form of a Declaration of Security between a ship and a port facility[8]

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 SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		

[8] This form of Declaration of Security is 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.

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 the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

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

Signed for and on behalf of	
the port facility:	the ship:
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*

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

Contact Details *(to be completed as appropriate)* *(indicate the telephone numbers or the radio channels or frequencies to be used)*	
for the port facility:	for the ship:
Port Facility Port Facility Security Officer	Master Ship Security Officer Company Company Security Officer

APPENDIX 2

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

(Official seal) *(State)*

Statement Number

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

The Government of_____
(name of the State)

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)

ENDORSEMENT FOR VERIFICATIONS

The Government of <*insert name of the State*> has established that the validity of this Statement of Compliance is subject to <*insert relevant details of the verifications (e.g. mandatory annual or unscheduled)*>.

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

1st VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

2nd VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

3rd VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

4th VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

***

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

25 February 2016

Mrs Shantal Ramsaroop 201292909
School of Law
Pietermaritzburg Campus

Dear Mrs Ramsaroop

Protocol reference number: HSS/0181/016M
Project title: Understanding the International Ship and Port Facility Security (ISPS) Code: An Examination of the Implementation and Effectiveness of the ISPS Code

Full Approval – No Risk / Exempt Application

In response to your application received on 24 February 2016, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....
Dr Shenuka Singh (Chair)

/pm

Cc Supervisor: Deepa lamb
Cc Academic Leader Research: Dr Shannon Bosch
Cc School Administrator: Ms Robynne Louw / Mr Pradeep Ramsewak

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za