Establishing an Appropriate Regulatory Framework and Harmonized Security Measures for the Protection of Mixed-Use Marine Facilities within Canadian Ports

By
Abdulraouf Hamrouni

Submitted in partial fulfillment of the requirements for the degree
of
Master of Marine Management

at

Dalhousie University
Halifax, Nova Scotia
August 2014

Table of Contents

Hamrouni, A. 2014. *Establishing an appropriate regulatory framework and harmonized security measures for the Protection of Mixed-Use Marine Facilities within Canadian Ports* [graduate project]. Halifax, NS; Dalhousie University.

Abstract

The significance of maritime transport security is a factor of the highly vulnerable and variable mode of maritime transportation and the resulting security threats from the various sources of cargo. There is an urgent need for nations to establish an effective security framework to resolve regulatory gaps and overlaps for their national security infrastructure within the marine sector. Several marine industries have been exempted from the scope of national and international security frameworks, notably the offshore oil and gas sector. Balancing the need for implementing suitable security measures with the need for sustainable trade objectives is a challenge for most countries. However, a consistent and comprehensive regulatory framework that addresses the majority, if not all, of the supply chain activities would reduce regulatory gaps, overlaps, thus ensuring that trade facilitation is continued. Implementation of a suitable regulatory framework for marine facilities' and ports' security could be founded on a public-private partnership, which would offer a collaborative and consultative environment for all stakeholders. It is expected that under this framework, marine industrial activity would be protected against any interruption resulted from security threats, while providing a clear and coherent regulatory framework. A case study of a proposed mixed-use facility in Richmond Terminal and Sheet Harbor, Nova Scotia, are used for a comparative analysis of their marine security regimes. Four international security infrastructure examples (i.e., Australia, United Kingdom, Canada, and United States) are additionally analyzed to propose lessons learned for improved marine security management in Atlantic Canada.

Keywords: Maritime security, critical infrastructure, offshore oil and gas, international examination, regulatory framework, marine management.

List of Abbreviations

AAPA--- American Association for Port Authorities

ACPA--- Association of Canadian Port Authorities

AEO--- Authorized Economic Operator

AIS--- Automatic Identification System

AMIS---Australian Maritime Identification System

AMSA--- Australian Maritime Safety Authority

AMSOC--- Australian Maritime Security Operation Centre

API--- American Petroleum Institute

BPC--- Boarder Protection Command

BSEE--- Bureau of Safety and Environment Enforcement

CBSA--- Canada Border Services Agency

CCG--- Canadian Coast Guard

CCPPP---The Canadian Council for Public-Private partnership

CDC--- Certain Dangerous Cargoes

CFN---CFN Consultants. Inc

CNS--- Commissionnaires Nova Scotia

CPAs-- Canada Port Authorities

CPNI--- Centre for Protection of National Infrastructures

CSCAP--- Council for Security Cooperation in the Asia Pacific

CSI--- Container Security Initiative

CSIS--- Canadian Security Intelligence Service

C-TPAT--- Custom-Trade Partnership Against Terrorism

DFO--- Department of Fisheries and Ocean

DFT---Department Of Transport

DHS--- Department of Homeland Security

DND--- Department of National Defense

DNV--- Det Norske Viritas

DOT--- Department of Transportation

EC--- European Commission

EEZ--- Exclusive Economic Zone

EU--- European Union

EU---European Union

FEMA---Federal Emergency Management Agency

FPSSD--- Facility Personnel with Specific Security Duties

FSO--- Facility Security Officer

GAMSA--- Guide to Australian Maritime Security Arrangements

GAO--- Government Accountability Office

GT--- Gross Tonnage

HPA--- Halifax Port Authorities

ILO--- International Labour Organization

IMO--- International Maritime Organization

IMSWG---Interdepartmental Marine Security Working Group

ISPS Code--- International Ship and Port Security

MARAD--- Maritime Administration

MCA--- Maritime Coastguard Agency

MCR--- Marine Commerce Resilience

MSA--- Maritime Security Awareness

MSGs--- Maritime Security Guards

MSIC--- Maritime Security Identification Card

MSLEP--- Maritime Security for Military, First Responder, and Law Enforcement Personnel

MSOCs--- Marine Security Operational Centers

MTOFSR--- Maritime Transport and Offshore Facility Regulations

MTRA---Marine Transportation Security Act

MTSCP--- Marine Transport Security Clearance Program

MTSD--- Maritime Transportation Security Division

MTSR---Marine Transportation Security Regulations

NMC--- National Maritime Centre

OCS--- Outer Continental Shelf

OMDUs---Offshore Mobile Drilling Units

OTS--- Office of Transport

OUMF--- Occasional Use Marine Facility

PPIC--- Public Policy Institute of California

RCC--- Regulatory Cooperation Centre

RCMP--- Royal Canadian Mounted Police

RO/RO--- Roll On/ Roll OFF

SAFE--- Security and Accountability for Every Port

SLA---Submerged Lands Act

SOLAS--- Safety of Life at Sea

STCW--- Standards of Training, Certification and Watch Keeping

TC--- Transport Canada

TSA---Transportation Security Administration

TWIC---Transportation Worker Identification Card

U.S. --- United States

UK--- United Kingdom

UN--- United Nation

UNCLOS--- United Nation Convention on the Law of the Sea

UNCTAD--- United Nations Conference on Trade and Development

USCG---United States Coast Guard

VPSSD--- Vessel Personnel with Specific Security Duties

Acknowledgements

I might not able to find the words to express my thanks and appreciation for those amazing people who contribute to this project. My completion of this project could not have been accomplished without this chain of well-educated, supportive, and kind people – starting with Becky Field, my supportive supervisor Dr. Hugh Williamson, Dr. Lucia Fanning, Dr. Elizabeth De Santos, Dr. Robert Fournier, and my host organization's staff of Halifax Port Authority. Thanks to all of my classmates and in particular Alexandra Vance, for all their understanding and collaboration the whole way. Thanks to my family for their unlimited effort to accomplishing this work.

1. Introduction

1.1. Maritime Security

The significance of maritime transport security is a factor of the highly vulnerable and variable mode of maritime transportation and the resulting security threats from the various sources of cargo. The marine transportation sector is diverse and complex; huge volumes of shipped cargo coupled with various logistics of people and goods, whose origin, ownership, and distribution may not be entirely assessed by marine security regulators around the globe (Papa, 2013). According to Huang *et al.* (2011), the future of waterfront development and uses will be further diversified, and that there will be an increasing need for international attention given to the protection and sustainable development of the coastline. Development of any port facility requires large investment; however, the payback period is usually longer and therefore requires investment to be continuous. The associated risks involved in developing port facilities often increase and must be mitigated with an effective public-private framework that focuses on the partnership and collaboration between all stakeholders, including the marine security authorities and legislators responsible for establishing marine security regulations. This mutually beneficial situation could be achieved with a strong investment partnership between both public and private sectors. The public sector lead by the various levels of government could offer regulations, laws, and jurisdictions; the private sector, likely composed of the operators and service providers of the marine facility, would offer trade opportunities, including the payback funds (Huang et al., 2011).

Given that marine security requires risk-based management, most of Canada's major marine ports and facilities have assessed their procedures based upon the International Ship and Port Security (ISPS) Code measures as incorporated within the Marine Transportation Security Regulations 2003. The development of a multiple-use and/or multiple-user port facility should

consider not only the economic benefits and the implementation costs but also appropriate security measures and regulations to avoid security interruption incidents, which would have negative impacts on the economy and the security of supply chain (Atlantic Gateway and Trade Corridors Strategy, 2010).

According to Transport Canada, the Canadian marine industry growth depends on its ports' and marine facilities' operation and management. Users such as private sector operators, including offshore oil and gas supply service, could be the best partners for its significant contribution to the global economy[1]. To facilitate trade, implementing security measures by operators and service providers is important and is required by the International Ship and Port Facility Security requirement or an equivalent governmental body (ISPS Code, 2003).

Resolving existing regulatory gaps and overlaps is crucial for the protection of the whole supply chain. Enhancing marine security regime requires authorities, legislators, and policy makers to establish consistent regulations that encompass marine industries' security requirements. Failing to do so would widen the existing gaps and create overlaps in the marine security which would become increasingly challenging to resolve them. Establishing an appropriate security framework for the protection of mixed-use marine facilities can be simplified if existing regulations have been properly reduced or filled. Exempted or unregulated marine related industries from the international and national regulatory frameworks represent vulnerability to security compliance. Governments, stakeholders, and decision makers must take the necessary measures to address and manage the security of unregulated marine industries and facilities; establishing suitable security regulatory frameworks for marine facilities would not guarantee effective, viable, and sustainable protection.

[1] Marine Transportation. Ports section. Transport Canada. Retrieved on July 15, 2014 from: http://www.tc.gc.ca/eng/programs/ports-index.html

1.2. International Overview

1.2.1. ISPS Code

In response to the terrorist attacks of September 11, 2001, the International Ship and Port Facility Security (ISPS) Code was adopted by the International Maritime Organization (IMO) in 2002 as a common regulatory framework to address securi[2]ty in international maritime transportation. International Ship and Port Facility Code (ISPS) is, "a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities" (ISPS Code, 2003). The mandatory and recommended requirements of the ISPS Code are implemented through chapters XI-2: special measures in Safety of Life at Sea (SOLAS) Convention. Given that ships and port facilities are considered risk management activities by IMO[3], governments are required to establish their regulatory framework to protect ships and port facilities from potential threats to maritime security (ISPS Code, 2003). Though the International Ship and Port Facilities Security (ISPS) Code was introduced, there is still the urgent need for countries to establish and enforce regulatory frameworks within their own jurisdictions. Ships and port facilities have left several marine related industries largely unregulated, such as fixed and non-propelled mobile offshore oil and gas installations and small vessels.

In July 2004, a new set of comprehensive security regimes were recommended by the IMO conference in London to adopt a number of amendments of comprehensive maritime measures to SOLAS Convention 1974. The conference also adopted a number of resolutions to encourage contracting governments to work on promoting maritime security in the future and to set an appropriate regulatory framework and legislative provisions for ships and port facilities that are not

---

2

[3] International Ship & Port Facility Security Code and SOLAS Amendments 2002 (2003 Edition). International Maritime Organization. ISBN 92-801-5149-5. Arkle Print ltd. London

covered by ISPS Code (ISPS Code, 2003). Part 2 of ISPS Code requires contracting governments to set the security levels appropriate for ships and port facilities. These security levels are:

- Security level 1 (MARSEC 1), normal: the level at which vessels and port facilities normally operates;
- Security level 2 (MARSEC 2), heightened: the level applying for as long as there is a heightened risk of a security incident; and
- Security level 3 (MARSEC 3), exceptional: the level applying for the period of time when there is the probable or imminent risk of a security incident (ISPS Code, 2003).

1.2.2. International Code of Practice on Security in Ports

In 2003, the international Labor Organization (ILO) collaborated with the Maritime Safety Committee of IMO to establish the code of practice to the security in ports. Establishing the code was a complementary step to the ISPS Code overall requirements for port security. ILO and IMO joint working group prepared the code with other representatives with interest in the development of the port security[4].

The objective of the International Ship and Port Security (ISPS Code) on security is to reduce risk that could result from unlawful acts and to help guide governments to develop and implement appropriate frameworks in a consistent and comprehensive approach amongst contracting governments to SOLAS measures (International Code of Practice on Security in Ports, 2003). The code offers additional requirements, measures, and further details not only for the port facilities but also to the port as a whole. It also provides a detailed method of identifying weaknesses in ports security by using the Threat and Risk Analysis Matrix. The code pays great attention to the importance of training and security awareness within the port, as well as the physical security of the

[4] The joint working group between ILO and IMO was established in 2003 by IMO Maritime Security Committee (MSC) based on IMO conference resolution 8 on enhancement of security in cooperation with International Labour Organization ILO. Please refer to http://www.imo.org/Ourwork/Security/Instruments/Pages/CoP.aspx Bill Waters, personal communication, September 13, 2013

port. Importantly, the code of practice is not aimed to replace or duplicate ISPS Code security approach for Port Facility Security Plans (PFSPs). However, it identifies the relationship with the port facility and provides the transition of marine security from the ship to the port facility into and from the port (International Code of Practice on Security in Ports, 2003).

1.3. Local Review (Port of Halifax Richmond Terminal)

The development of any port facility requires a large investment; in the case of the port of Halifax Richmond Terminals, the development plan included $73 million of shared federal and Halifax Port Authority (HPA) funds. The Port of Halifax is one of the major seaports within Canada; its activities economically contribute $1.58 billion in gross output and $671 million in gross domestic products. The port is responsible for approximately 11,000 employment opportunities to the Province of Nova Scotia. The navigable waters of Halifax Harbor, under the management of the HPA, extend from the harbor limits to the end of Bedford Basin and also include the Northwest Arm.

According to MTSA and its regulations, Canadian marine facilities security has been addressed in part 3 of the regulations in terms of operators' responsibilities, requirements, certifications, security assessment and plans. MTSA defines marine facilities as, "an area of land, water, ice or other supporting surface use, designated, prepared, equipped or set apart for use, either in whole or in part, for the arrival, departure, movement or serving of vessels"[5]. This definition includes buildings, facilities, and equipment's used to provide services related to marine transportation. The operator of the marine facility is responsible for the management and control of the facility, regardless if it is an owner or an agent for the owner. The liability or costs incurred by Transport

[5] The Canadian Marine transportation Security Act 1994 in the interpretation section defines marine facilities as quoted above. Please refer to Canada Marine Transportation security Act (1994). Justice Law Website, S.C. 1994, c.40. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/M-0.8/FullTextAustrali.html

Canada (TC) in carrying out security measures is identified by the MTSA as the operator. According to the Association of Canadian Port Authorities (ACPA, 2004), port authorities are additionally accountable for planning and conducting security assessments, but without liability. The MTSA requires the operator of the marine facility to carry out the security measures for their facilities in section 7 (a) of the Act, and gives the minister of TC the right to carry out security measures on marine facilities where the minister considers that the security measure of goods and people are not properly protected in section 8 of the MTSA.

The Canadian MTSR is among the only the maritime security regulations that have a provision for Occasional Use Marine Facility (OUMF). According to MTSR, the OUMF is defined as, "a marine facility that, in a calendar year, has 10 or fewer interacts with vessels to which part 2 of MTSR applies where no more than 5 of those interacts involve a vessel on a fixed schedule with the facility". Based on this definition, TC inspectors have the criteria to classify and approve marine facilities security certificate of compliance. TC to enhance the maritime security regime within Canada, by addressing small and/or local marine facilities security requirements made such provisions. Interestingly, the classification criteria considers the trend of the number of vessels interacting with the marine facility in order to determine its statement of compliance. The advantages and disadvantages of the OUMF's marine facilities requirements and responsibilities are discussed (see section 3.3).

1.4. Compliance Issues

1.4.1. Background

Interruption in the maritime supply chain would have negative impacts on the whole marine transport process. To establish a proper regulatory framework for the security of mixed-use port facility, a number of regulatory issues need to be resolved in order to achieve a reliable, effective, and consistence regulatory framework. Marine industries, such as offshore oil and gas installations,

non-marine industries, and a range of small domestic vessels, are often not properly managed in terms of their security[6]. If the security activity fails, it will surely impact the competiveness of the global marine transportation supply chain (Banomyong, 2005). Building a strong partnership between public and private sectors would help to ensure a secure supply chain and economic benefits for all involved stakeholders. There is a need for more research such that there are some regulatory gaps and potential jurisdictional overlaps that could negatively affect the establishment of suitable regulatory frameworks for the security of mixed-use port facilities within Canada. Before establishing or implementing any security arrangements, addressing the existing gaps and overlaps is an important step to ensure the sustainability and consistency of the maritime security regime and trade. Having clear and inclusive regulations would be important for marine industry so to be able to facilitate trade within a well-protected environment. Unregulated and noncompliant marine industries pose a threat to marine transportation and supply chain security. Establishing suitable security frameworks for marine facilities would not necessarily guarantee the facility will be as protected as it should be, unless noncompliant and unregulated marine industries security has been included within the overall maritime security regime of Canada.

1.4.2. Regulatory Gaps

According to UNCTAD analysis framework for compliance measurement and risk assessment (2006), maritime security management must take into account the complex regulatory and operational aspects of the maritime industry operations[7]. The current security framework and

[6]Many contracting governments to SOLAS Convention have excluded small vessels under 500 GT and fixed offshore oil and gas installations from their marine security regulations such as United Kingdom and United States. Others did include small vessels under 500 GT in their maritime security regulations such as Canada. Australia as well has included offshore installations in its maritime security framework.

[7] Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment, (2006). United Nations, New York and Geneva, 2006. UNCTAD/SDTE/TLB/2005/4. Retrieved from: UNCTAD.org/en/Docs/sdtetlb20054_en.pdf

security assessment application should be extending not only to cover marine facilities, ports, and vessels but also the whole supply chain and its security to avoid any regulatory gaps, create more consistent and coherent maritime security regimes, and promote competitiveness.

The main regulatory framework for the maritime security in Canada is the *Marine Transportation Security Act (MTSA)* and its regulations. Under this act, Transport Canada has the authority to regulate security in Canadian ports (Transport Canada, 1994). Like the ISPS framework, the Marine Transportation Security Regulations (MTSR) has explicitly excluded non-self-propelled Mobile Offshore Drilling Units (MODUs), fixed offshore installations, and small vessels (e.g., pleasure crafts, fishing vessels, and vessels under 100 gross tonnages) from their scope of application.

1.4.3. Jurisdictional Overlaps

In April 2011, the Chief Safety Officer of Canada Nova Scotia Offshore Petroleum Board issued a safety directive to address security issues along Nova Scotia for specific measures for offshore installations and ships that are not covered by the ISPS Code. The Nova Scotia Offshore Petroleum Board has recommended the security for worldwide offshore oil and natural gas operations in accordance with subsection 70(I) of the American Petroleum Institute (Canada-Nova Scotia Offshore Petroleum Board, 2011)[8]. On the other hand, Canada's Newfoundland and Labrador Offshore Petroleum Board legislation requires offshore facilities including drilling units and platforms must perform security assessments and plans as required by the ISPS framework. The security requirements are in agreement to subsection 51(3) of the Newfoundland Offshore Area Petroleum Production and Conservation Regulations (Development Plan Guideline, 2006). Despite this, gaps and overlaps remain observable within Canada's maritime security regime.

[8] Canada-Nova Scotia Offshore Petroleum Board Safety Directive (2011). Security of Offshore Installations and Facilities. Canada-Nova Scotia Offshore Petroleum Board. File No 20,100.11. Retrieved from: www.cnsopb.ns.ca/pdfs/Security_Directive.pdf.

1.5. The Project's Plan and Purpose

The main purpose of this project is to conduct an overview on the selected national and international regulatory frameworks to address any regulatory gaps and or overlaps that may arise during the operational security within mixed-use port facilities and ports. Besides unregulated marine related industries facilities, there is evidence that some of the marine industries within Canadian and international maritime security regimes are not fully compliant with the national and international regulatory framework for maritime security[9]. An overview on different nations' approaches on how to manage security within their maritime security regimes would be a step towards establishing a proper security regulatory framework for Canadian marine ports that are aiming to benefit from utilizing their facilities as a mixed-use marine facility.

It is expected that reducing regulatory and jurisdictional gaps and overlaps would become the foundation for establishing an effective, reliable, and sustainable regulatory framework for the security of mixed-use marine facilities. Enhancing the security by creating more consistent and comprehensive regulations may result in additional costs for marine users, operators, vessels, and service providers; however, provided that marine industries could adapt to greater costs if they were given ample time for implementing the regulations. Contrastingly, a well-protected maritime supply chain would definitely facilitate trade and increase competition, which could be economically beneficial to the chain. To best implement suitable security measures, it is important to promote the consultation, collaboration, and understanding between government and stakeholders. The principle of public-private partnership is a key issue to promote stakeholder maritime security awareness (Papa, 2013).

[9] Within Canada, the security of fixed and non-self-propelled offshore oil and gas installations is not properly managed and regulated. While C-NSOPB has a set of security measures (American Petroleum Institute 70 guideline), C-NFLOPB has a different set of security regulations by implementing ISPS code measures as required by the memorandum of understanding between the Federal Government and the Board.

2. Methodology

2.1. Case Study Selection

Halifax Port Authority has proposed to utilize the upgraded Richmond Terminal as a mixed-use marine facility. This mixed-use marine facility would encompass a major port in which various operators interact with one other, and different marine industries interact within the same terminal at the same time. As a result, this is a suitable case study to examine the effectiveness of the regulatory framework for the security and any regulatory gaps or overlaps within the port's operational security regime.

To assess Richmond Terminal mixed-use marine facility case study in an international context, an overview on four nations' (i.e., Australia, Canada, United Kingdom, and the United States) regulatory frameworks for port security provided a set of security practices and measures that could be recommended for Canadian Port Authorities. The purpose of this assessment was to understand the roots of the regulatory issues and how to overcome these problems in order to best manage the operational security in Canadian ports. These four nations have among the most advanced and comprehensive marine security regulatory frameworks worldwide, as well as maritime security regimes being comparable to one another in terms of the regulations, organization structure, authorities, and initiatives of marine security. There are also some similarities between these countries in terms of geography, political stability, and marine industries and uses.

2.2. Case Study Analysis

A range of sources used to obtain the information for this paper, including library books and online journal articles focused on maritime security and port development. Several articles were retrieved from Google Scholar, and an overview on different official government websites examined the respective regulations and initiatives. Additionally, a number of people related to

marine security were consulted to generate ideas and discuss the existing regulatory gaps and overlaps; the people whose consultations contributed to this project are:

- Bill Adams from Atlantic Towing Management Department on July 2014;
- Pamela Brennan, Transport Canada Inspector meeting on June 2014;
- Patrick Bohan HPA Manager Business Development on May 2014;
- Diedre Lewis, HPA Manager of Marine Operations on May 2014; and,
- Aaron Dickson, HAP Security Officer on May 2014.

2.3. Limitations and Scope

This project had originally been envisioned to focus on offshore oil and gas security frameworks; however, such a project was not possible to complete due to strict security regiments and an inability to achieve security clearance to access critical information. The resulting scope of this project instead focused on the linkages between offshore oil and gas industry with various port and marine facility security approaches. This newly envisioned project was equally desirable to investigate given the number of the marine activities and interactions occurred within these facilities.

Again due to the confidentiality of security information, access to information regarding ports' plans and assessments was limited. In accordance with section 366D and E, MTSR requires that port and facility security managers keep such information protected from unauthorized access or disclosure. Although this limitation may affect the accuracy and credibility of this project's scope of research, the project has largely adopted a generic methodology for security information sourcing for the examined ports and marine facilities. Additionally, the limited amount of time to complete this project imposed a challenge since addressing regulatory gaps required more time for research and investigation.

3. Richmond Terminal Case Study

3.1. Port of Halifax Richmond Terminal

Once completed, the terminal will cover 77.2 square kilometers and a maximum depth of 9.1 meters with the ability to accommodate rail and truck access areas. It contains five berths that can handle break-bulk, offshore supply, heavy lift, and containers. This project is one of the Mega Projects of Atlantic Canada Gateway with $73 million of shared costs between the federal government and HPA[10]. It is prepared to handle trade associated with the Comprehensive Economic Trade Agreement with the European Union, and other local projects such as the National Shipbuilding Procurement Strategy and Offshore Oil and Gas Industry. The approach taken by HPA is to allow for increased growth in the break-bulk cargo by developing capable and well-protected facilities within the port (HPA Stakeholder Report, 2013).

At the time of this report, the terminal was in the construction phase of development, and is classified as an occasional-use marine facility. The security perimeter of the new terminal and its facilities is still under review between HPA and TC inspectors. Once the project is completed, HPA would have to submit the security application to TC for an approval certificate of compliance. Upon reviewing the security measures and vessel trends, the decision will be made to determine the status of the marine facility. Due to the construction work, the terminal has not reached the minimum number of required interactions, which would affect the resulting approval certificate of compliance.

3.2. Sheet Harbor Terminal

Sheet Harbor is a multi-purpose marine facility, ice-free, with 10 meters minimum draft, located in the Eastern Seaboard of Nova Scotia. Its strategic location provides access by trucks and

[10] Gateway Infrastructure Projects in Port of Halifax. Please refer to www.portofhalifax.ca/port-facilities/infrastructure/

ships to anywhere within North America. Moreover, it is only 80 Kilometers from the Great Circle Route between North America and Europe, meaning that it has among the shortest sea route for ships. Its wharf is 152 meters long, including the MARSEC secured 12 acre common-user layout area adjacent to the wharf. The wharf can handle various cargos such as break-bulk and special project cargos. It is also an attractive destination for trade because of its access to highways, cost competiveness services, and capable handling stevedores. It used to be classified as an occasional-use marine facility in TC's list of ports compliance program[11]. However, HPA recently has applied for a fully compliant marine facility; HPA has submitted its security assessment and plan to TC and it is expected that TC will approve the plan due to a recently increased trend of vessels visiting the terminal (HPA Security Officer, 2014).

The security procedures implemented at Sheet Harbor are in accordance with MTSR in sections 355-358 for occasional-use marine facilities. A declaration of security is required in each interact and most of the security duties occur during the interaction with visiting vessels. Due to the recent small number of vessels visiting the terminal, the type of cargoes handled, and its location in rural area of Nova Scotia, the terminal is less vulnerable to security threats. However, the vessel log of Sheet Harbor in 2013 has shown that the number of vessels is increasing which may require more security operations and activities.. These trends show that 12 vessels were interacted within Sheet Harbor in 2013, which is more than the limits established by TC for occasional-use marine facilities status. The trend also shows that from January to July 2014, there were 7 vessels that already used the terminal. Based on this trend HPA has submitted a security assessment and plan to TC to have the status of a fully compliant marine terminal for Sheet Harbor Terminal. Asides from the security aspects, the terminal is a small multi-purpose marine facility with no adjacent critical infrastructures. In most cases, there will be just one vessel at the berth, ensuring that simultaneous

[11] Sheet Harbour Specifications and information (2014) obtained from Patrick Bohan HPA Manager Business Development on May 2014. Specifications of the Port Sheet Harbour could be requested from HPA Business Development and Operations Department.

interaction or intervention with other operators or authorities responsible for maritime security would not occur. That is not to say that threats are not possible, but the likelihood of risk is expected to decrease as a result of fewer interactions. As a small multi-purpose marine facility, the regulatory gaps and potential authority overlap are easy to deal with; for instance, threats of interacting offshore supply vessels that are coming from unregulated offshore oil and gas installations could be mitigated. A declaration of security between the vessel and the marine facility and other regular security procedures could be implemented. Security guards would be assigned to guard the vessels during the entire tenure of the interaction.

3.3. Ocean Terminals

The terminal consists of two piers with access to train rails and trucks. This 200,725 square foot area is equipped with storage capacity and capable of lifting and break-bulk cargos. It is also a fully compliant facility with MTSR and ISPS Code regulations. The access control to the terminal facilities (i.e., Vascular Scanning) is one of the most advanced security technologies in the world. Commissionaires Nova Scotia (CNS) provides HPA with trained personnel whom have the capability to operate security operations within the port area of jurisdiction[12].

The terminal is a fully compliant marine facility with the national requirements of MTSR and the international security framework ISPS Code. The security plan involves a dedicated 24 hours on-site police service and technology that makes these ocean terminals one of the most well protected marine facilities within Canada. This port is currently assessed as MARSEC Level 1, and the port still operates under the normal operations.

In 2007, Dalhousie University hosted a forum for sharing views and information about critical infrastructure protection. One of the concerns from the forum was balancing security and efficiency

[12] Commissionaires Nova Scotia has been designed by the Canadian Group of Commissionaires to provide training courses and trained personnel as required by Canada Marine transport security regulations 2004 for ports and marine facilities employees including Halifax Port Authority. Pleas refer to commissionaires.ns.ca/?page_id=701

of the Port of Halifax. Giving that the ocean terminal is one of the Port of Halifax complex marine facilities involving cargo infrastructure, power generation, and tourism, the port has deployed a vascular scanning system that is capable of detecting blood flowing through the veins in the back of one's hand. Such advanced technology is one of the newest security measures for access control used in the ocean terminal (Critical Infrastructure protection exchange forum, 2007). Adjacent facilities and infrastructure are well protected by fencing, guards, and monitoring cameras, and gates control access between the ocean terminal and South End Container Terminal.

3.4. Comparison of Sheet Harbor and Richmond Terminal

The purpose of this comparison is to identify the MTSR used for the provision of occasional-use marine facility in its regulations, and to address the regulatory gaps that could be resulted from such a provision. First, this section will discuss what is the main purpose of establishing such a provision, whether it is to address non-regulated or rural marine facilities, or is it a transitional status from non-compliant to fully-compliant marine facilities. It may also be to address the security benefit of having marine facilities that do not have security measures or plans in place. It cannot be said that OUMF are fully-compliant since they do not require security management. According to TC list of ISPS Code compliant Canadian Marine Facilities and Ports as implemented by MTSR 2004,, OUMFs should have security procedures in place and no security plans are required. Therefore OUMFs are not fully-compliant with ISPS Code because they do not require security plans which are important to manage security of marine facilities[13]. The issue therefore is when port administration is fully-compliant with MTSR and ISPS Code, such as HPA, and attempting to establish a marine security plan for their facilities since they will be facing the inspectors' criteria for marine facilities, including the number of vessels interfacing with the marine facility. In this

[13] TC has a list of ISPS Code compliant Canadian Marine Facilities and ports as implemented by Marine Transportation Security Regulations. The list contains ISPS Code compliant facilities and MTSR compliant facilities. Please refer to http://www.tc.gc.ca/eng/marinesecurity/information-compliant-92.htm

case, regulations will dampen business and development goals of the ports' industries and create greater complexity when handling the aforementioned issue since it will result in degrading security and integrity of the port as a whole as well as the sustainable development objectives for the country[14].

3.4.1. Operators

The operator of an occasional-use marine facility must ensure that the requirements of sections 315 (Declaration of Security) and 355-358 of the Marine Transportation Security Regulations are met. There are 6 similar tasks and 4 additional tasks for the fully-compliant marine facility; these 4 additional tasks require the operator to operate the marine facility in compliance with the marine facility security plan and make any corrective actions to address the detected deficiencies. It is also required to submit the security assessment information mentioned in section 317 to the minister. However, if the occasional-use marine facility operator is in a port, the security officer of the occasional use marine facility should participate in the port security committee to ensure that the marine facility security has been developed as needed (MTSR, 2004)[15].

3.4.2. Qualifications

According to MTSR, the qualifications required by the fully-compliant Marine Facility Security Officer (MFSO) are higher than OUMF security Officer such that they are required to have experience, approved training, and knowledge of conducting inspections, on-site surveys, and marine facility security assessments. MFSO should be qualified to conduct physical searches, training drills and techniques within the marine facility and the vessels, as well as the capacity to operate and maintain security equipment, including communication devices. Moreover, the MFSO

[14] Within the area under HPA administration, there will be different marine security operations. OUMFs have no security plans as per MTSR, while ISPS Code full-compliant marine facilities have. These security requirement differences may have negative impacts on security and development of the port.
[15] Please refer to Canada MTSR 2004 in the references list.

should be able to recognize behavioral patterns of personnel and have knowledge of how to recognize security threats and detect sources of risk; all these qualifications require approved training courses by TC[16]. Meanwhile, occasional-use MFSO qualifications do not require security officers to have training or knowledge on how to conduct physical searches, nonintrusive inspections, crowd management or techniques that could prevent the violation of security, such the use of Certain Dangerous Cargoes (CDC) as a weapon.

3.4.3. Responsibilities

There are mainly three similar responsibilities for occasional-use and fully-compliant marine facilities officer, namely; 1) ensuring security awareness of any circumstances that might threaten the marine facility is important duty for occasional-use and fully-compliant marine facility security officers, 2) the officer is also responsible for making sure that training for personnel is provided, and 3) reporting security incidents to the law enforcement authority is a shared responsibility for both occasional-use and fully-compliant marine facilities[17]. However, for occasional-use marine facility security officers, security sweeps should be performed before and after the ship-port interaction and to keep record of the security sweeps. Also, the declaration of security should be made following the security sweeps, and the security officer should send all reports to the Minister. For a fully-compliant marine facility, the facility's risk assessment should be made and the security plan should be submitted to the Minister for approval. Breaches of security or security deficiency in the marine facility security plan should additionally be reported to the Minister upon their correction. Ensuring reliable and effective communication between the facility and the vessel is important to facilitate good communication during the interaction and communicate any changes in the security levels. The results are there is no security assessment or plan required for occasional

[16] Please refer to Canada MTSR 2004 in the references list.
[17] Please refer to Canada MTSR 2004 in the references list.

use marine facility which makes it more vulnerable to security threats because security procedures required for occasional-use marine facility are not as intensive as the security plans. A declaration of security is an agreement between the vessel and the marine facility before the interaction. It is required by occasional-use marine facilities before each interact with vessels. However, for fully-compliant marine facilities, it is required under conditions stated in section 228 of the MTSR.

The advantages of establishing OUMFs within Canada is that it allows more flexibility to vessels to interact with non-fully compliant marine facilities, reduces costs associated with establishing marine security measures and plans, and MFSOs' requirements and certifications. It also addresses small marine facilities that are located in rural areas. On the other hand, this provision gives more flexibility for marine transportation users and facilities, which increase managerial gaps and inconsistency of the overall maritime transportation security regime of Canada. Although interacting with occasional-use marine facility can be a large expense, vessels prefer to interact with fully-compliant marine facilities that provide confidence to vessels that are covered right up to the end of the gangway (Adams, 2014)[18]. The interaction with occasional-use marine facilities could be expensive because vessel operators have to pay the security guards controlling the access to the vessels. It would also create more security issues and conflicts, especially for marine facility users within the same port or area.

3.5. Vessel Trends

The vessels that utilized Richmond Terminal between 2012 and 2013 have shown trends of an increased number of interactions, even during the construction and upgrading development. In 2012 there were more than 40 visits to the terminal; in 2013 there were more than 60 interactions. Most of the vessels visiting Richmond Terminal are under the category of miscellaneous, fishing, and offshore supply vessels (HPA statistics department, 2014). Therefore, the issue is that even with the

[18] Bill Adams, Atlantic Towing, Personal Communication, June 2014.

increased number of vessels utilizing the terminal, the terminal is still classified as an occasional-use marine facility. Part of the criteria of this classification is that most of the vessels visiting Richmond terminal are beyond the scope of the ISPS Code and MTSR frameworks, which certainly have the propensity to create a regulatory gaps which need to be addressed by the appropriate security authorities. Domestic and small vessels security should be given more attention by marine security legislators because each vessel (International and Domestic) interacting with marine facilities represent security potential threat.

4. International Comparative Analyses

4.1. Australia

4.1.1. Overview

Following the American tragedy of September 11, 2001, Australia had shifted its marine security management from civil dimension security approaches to a formal defense policy. Australia has a 34,000 km of coastline and extensive offshore territories and values; in 2009, the value of seaborne trade was approximately $368 billion, exports were valued at $202 billion, and imports were valued at $166 billion (excluding both the economic and employment values) with oil and gas exploration and production valued at $9.8 billion that year. Australia has more than 70 commercial ports that handle approximately 51.6 million tons of domestic trade alone, and export 99% of Australian productions (Forbes, 2011). According to NOPSEMA, there were 149 active offshore facilities including pipelines, fixed and mobile platforms in 2013.

4.1.2. Regulatory Framework

In 2003, the Maritime Transport Security Act (MTSA) was introduced into Australian marine security regimes to implement the ISPS Code. To meet ISPS code requirements, the act came into force on July 2004 and was applied to Australian ports, port facilities, and ships. Due to international development and a national need for an enhanced and formalized approach for operators to better regulate for the offshore oil and gas installations, the Australian Government extended the Maritime Transport Security Act 2003 to include Australia's offshore oil and gas facilities in 2005, then renamed the Act as the *Maritime Transport and Offshore Facilities Security Act* (MTOFS Act) (Maritime Transport Security Amendment Bill, 2005*)*This newly amended act required that all maritime industry participants (e.g., ports, offshore facilities and service providers) to assess and combat potential risks in the maritime industry by undertaking security assessments

and implementing security plans. Marine industry participants within the Australian maritime security regime should also undertake measures at different security levels, report incidents, and utilize screening technologies designed for detecting prohibited items (Australian Government Department of Infrastructure and Regional Development). Such security plans and measures are subject to regulatory approval and ongoing enforcement, and are supported by legislative measures such as control zones, maritime security identification card, private security personnel, and criminal offence provisions (GAMSA, 2013).

4.1.3. Organizational Structure

Australia marine security is a multi-agency approach, consisting of 12 commonwealth agencies (Bateman, 2007). The Australian maritime security regime is implemented by the Department of Infrastructure and Regional Development Ministry through the Office of Transport Security (OTS). OTS is the key principle of managing the security within Australia's shipping sector, including ports and offshore industries, and implementing ISPS Code requirements. The primary objective of the OTS is to protect Australian maritime transportation systems and offshore facilities' activities against terrorism and unlawful acts; however, the lead agency for maritime terrorism threats in Australia is the Border Protection Command (BPC) The National Counter-Terrorism Plan of the Australian government has the responsibility to counter terrorism threats from the near-shore coastal zones to the offshore zone, extending as far as the limitations of the EEZ and continental shelf. However, the provinces have direct responsibility for preventing and responding to threats within their internal waters and port limits (GAMSA, 2013).

4.1.4. Major Initiatives

4.1.4.1. Maritime security Guards and Maritime Security Identification Card

One of the mitigation security measures of the *MTOFS Act* 2005 is the introduction of Marine Security Guards (MSGs), which are responsible to perform access control, monitor restricted areas, and screen cargoes, as well as the ability to restrain and attain people. The Maritime Security Identification Card (MSIC) is a security card required by port, port facilities, stevedores, and seafarers on Australian regulated ships and offshore workers who work in a maritime security zone. However, the MSIC is not an access card to ports or marine facilities; rather, it is an operational and/or business unmonitored access for business needs (Department of Infrastructure and Regional Development, 2014).

4.1.4.2. Maritime Security Operation Centre

One of the most recent initiatives of Australian maritime security development is the Australian Maritime Security Operation Centre (AMSOC), which was established and operated by the Australian Custom and Border Protection Agency (ACBPA) to manage the overall operations throughout the year. The ACBPA coordinates the planning of operational activities for border protection (e.g., deploying aerial and surface responses to maritime security threats) and has embedded officers from several agencies (e.g., fisheries, safety, and border protection) to better facilitate the operation of maritime security (Australian Border Agency Annual Report 2008-2009). As part of the Border Protection Command, AMSOC has the responsibility to manage Australian Maritime Identification System (AMIS), which is one of the latest Australian initiatives introduced in 2009 to better integrate information about maritime threats to enhance Australia maritime security approaches (BPC Fact Sheet, 2009).

4.1.5. Offshore Regulations

Australia's offshore oil and gas security framework was introduced in 2003 in order to protect domestic and international sea trade, which is regulated by the Australian government to make security arrangements for Australian ships, ports, and ports facilities. The need for establishing a legislative framework for security plans for offshore oil and gas facilities has led the Australian government to amend the act to meet such requirements. Therefore, the *Maritime Transport Security Act* 2003 (MTSA) was renamed in 2005 to the *Maritime Transport and Offshore Facilities Security Act* 2005. This amendment is the responsibility of the Office of Transport Security for Implementation and Assessments of Offshore Oil and Gas Facilities Security Plans. The Australian Transport Security office requires that offshore facility operators and service providers must have an offshore security plan in force, even if the maritime industry participant is not required to have one. Similarly to the United States, the Australian approach for securing offshore oil and gas platforms is a proactive (Avis, 2006). Interestingly, part 6 of the *Australian Maritime Transport and Offshore Facilities Act 2005* details that the offshore security zones must be clearly identifiable with access controlled. The Department of Infrastructure and Transport has issued a Guidance Paper on Signage and Notices to assist maritime industry participants to meet these obligations to better inform the public of the whereabouts of maritime security zones and that they are enforced for for ships, ports, ports facilities, and offshore oil and gas facilities(Australian Department of Infrastructure and Transport, 2013).

Australia implemented the AMIS in 2004 as a system that would require ships transiting in the Australian EEZ to provide logistical information, such as crew, cargo, and intended port of entry (Harel, 2012). The Australian strategy for enhancing offshore security was based on the premise that the level of threat posed by terrorists could be reduced by deterrence (Avis, 2006). To do so, the Australian government gave the Australian BPC and the Defense Force the responsibility to

encounter offshore terrorism. A number of initiatives such as the AMIS augmented security patrols, and the Joint Offshore Protection Command was implemented (Avis, 2006).

4.1.6. Small Vessel Regulation

To comply with the *Maritime Transport and Offshore Facilities Security Act 2005*, Australian security agencies have since regulated ports, service providers, and marine facilities, which are required to follow the responsibilities and guidance materials provided by the Department of Infrastructure and Transport. The Australian authorities responsible for implementing maritime security regulations stresses the importance of maritime security plans for maritime industry participants even when such plans are not required. The Department of Infrastructure and Transport states that, "it is an offence for a maritime industry participant to operate without a maritime security plan in force when one is required"[19]. Moreover, maritime industry participants such as port, marine facilities operators, and service providers are also subject to the authority enforcement when they obstruct security plan compliance of another participant. The *Maritime Transport and Offshore Facilities Security Act 2005* has given ports, marine facilities, and offshore facilities the obligation to establish their respective maritime security zones to cover the landside, waterside, and clear zone (Australian Government Department of Infrastructure and Regional Development, 2014). Under the *Maritime Transport and Offshore Facilities Security Act 2005,* the Department of Infrastructure and Regional Development issued a preventative security guideline for cruise ship visits to unregulated places in response to the departments realizing that terrorists will seek out security weaknesses by observing how businesses deal with security measures in order to select

[19] The Australian Department of Infrastructure and Regional Development requires maritime participants to have security plans in force. Maritime participants are; operators of security-regulated ports, operators of facilities at security regulated ports, and providers of service at such port. However, the department considers it an offence for maritime participants to operate without security plans in force. If they are not required to have one, they must not hider compliance with the security plan of another participant. Please refer to http://www.infrastructure.gov.au/transport/security/maritime/security_plans/port_operators.aspx

their possible targets for terrorism[20]. However, occasional-use marine facilities' operators are required by this guideline to conduct risk assessments, and the operators should consider geography, proximity to population, infrastructure, among other factors when conducting the risk assessment. The basic preventative security measures required by the guideline are 1) basic physical security, 2) detection and resolution of suspicious activities, and 3) human factors.

4.1.7. Marine Security Training

The Navigational Safety and International Division of the Australian Maritime Safety Authority is the primary responsible for providing strategic advice on maritime safety and security. Its responsibility includes representing Australian government in IMO for the implementation and enforcement of international standards of maritime security and training management. For seafarers training and certification, including Ship Security Officer and Security Awareness, the Australian Maritime Safety Authority (AMSA) is responsible for the endorsement and approval of training certification. AMSA has a list of approved institutions for providing security training; however, it does not endorse or promote specific institutions or courses. The department of Infrastructure and Transport has the primary authority responsible for implementing the Maritime Transport and Offshore Security Regulations has an oversight role in relation to advising Australian Maritime Safety Authority about government maritime security policiers and matters. Ironically, the most important requirements of training in accordance with MTOSR (in sections 12.2 and 17.2

[20] Please refer to Australian Government Department of Infrastructure and Regional Development Preventative Security Guidance for Cruise Ship Visits to Unregulated Places. Preventative Security Guidance for Cruise Ship Visits to Unregulated Places. Australian Government Department of Infrastructure and Regional Development. Accessed on July 24, 2014. Retrieved from: https://www.infrastructure.gov.au/transport/security/maritime/files/preventive_security_guidance_for_cruise_ship_visits_to_unregulated_places.pdf.

of ISPS Code part A) are that the duties and responsibilities of ship and port facilities' security officers should be provided by Australian-approved AMSA institutions (MTOSR 2003).

4.2. United Kingdom

4.2.1. Overview

As an island with roughly 12,500 km of coastline, the United Kingdom (UK) relies on maritime trade for about 95% of total trade. The UK has approximately 120 commercial ports that handle over half a billion tons of goods annually (Department for Transport, 2011).

4.2.2. Regulatory Framework

The UK maritime security regime was outlined by the *Aviation and Maritime Security Act* 1990. By 2002, ISPS Code was incorporated by the European Commission (EC) into the Directive 725/2004 on enhancing ship and port facility security regulations. The EC regulations were transposed into the UK regulatory framework for maritime security by introducing the Ship and Port Facility Regulation 2004, and its respective amendments in 2005. Interestingly, the EC made some of the ISPS Code's part B recommended regulations into mandatory requirements for implementation. One of the major European Union (EU) initiatives on maritime and port security is the Pre-Arrival and Pre-Departure Program. The EU's Authorized Economic Operator (AEO) 2008 is a mandatory program for member states in order to identify reliable traders and facilitate custom controls resulting from any disruption events.

4.2.2.1. EC Directive 65/2005 on Enhancing Port Security

The implementation of the EC Directive 65/2005 on Enhancing Port Security came into force on June 15th, 2007. It is a pursuant step to the EC regulations on enhancing ship and port facility security regimes of 2004 known as (EC) No 725/2004 Directive. The European Parliament and the Council of the European Union have recognized that the scope of the EC regulations on enhancing

ship and marine facility security was limited to address only security measures onboard ships, and during the interactive ship-port activities. To fulfill maritime security protection measures throughout the maritime transport chain, the EC Directive on enhancing port security has given guidelines for port industries such that necessary security measures should be implemented in all European ports. The directive is mainly focusing on security assessments, identification of potential threat areas, security plan appropriateness and measures, and basic security training requirements. Importantly, the directive requires that states' security assessments should, where useful, subdivide the port according to the likelihood of security incidents, and that port areas should be assessed based on their potential role of access or passage, variations, and seasonality. Although cargo control access requirements may or may not apply to sub-areas, the security plans should consider the need for technical solutions when monitoring activities within subdivided areas of the ports (EC Directive 65/2005).

4.2.2.2. The Port Security Regulations 2009

The UK's Port Security Regulations were established by the Secretary State of Transport and came into force on September 1st, 2009. The secretary of transport realized the necessity for certain provisions of the ISPS Code to be integrated in the maritime legislation and regulation of the European Commission 725/2004 on enhancing ship and port facility security. The regulations have 6 main parts, including: part 2 for Port Security Authority, part 3 for Port Security Officer, part 4 General Requirements for Port Security Assessment and Plan, part 5 for Controlled Building and Restricted Areas, and part 6 for Enforcement. The regulation in part 2 gives the port security authority the right of objection on decisions related to changes or amendments to the security plan of the port and any changes in charging fees. It also provides the port security authority and the port security officer the power to require information from port facilities' security officers or managers related to the function of their security measures. The port security authorities must submit the

security assessment reports for the port, port facilities, and any area adjacent to the port to the Secretary of Transport. The port authority security plan and assessment must be reviewed within 30 days of any major operational and structural changes in the port. Schedule 3 of the regulations requires detailed security information to be considered in the security assessment, including that it must identify all areas that are relevant to port security. Additionally, identified areas for potential security threats focus not only on their potential targets, but also upon their potential role in passage, as well as identified vulnerability of the overarching port security related to legislative and procedural aspects (The port Security Regulations, 2009 No.2048).

4.2.3. Organizational Structure

The Department for Transport is the primary responsible for the National Maritime Security Program in the UK. The department implements security measures to ensure that all security arrangements meet UK standards for ships and ports. The Maritime Coastguard Agency (MCA) is the agency responsible to the department for Transport for implementing ISPS Code for all UK registered ships and ports. The Security Policy Branch within the MCA coordinates a set of special measures to ensure the security in the maritime community. The Branch also provides technical advice and guidance to make sure that ISPS Code is implemented and maintained. The MCA is also undertaking security aspects of Port State Control Inspection and approving training courses' providers for ship security officers, company security officers, and port facility security officers (MCA, Ship Security, 2013).

4.2.4. Major Initiatives

4.2.4.1. The National Maritime Security Committee

To facilitate consultation on strategic maritime security issues with the maritime industry, DFT has established the National Maritime Security Committee. A variety of port, shipping, and other

departments' representatives meet twice a year to provide the maritime industry with consultation on shipping and ports operational matters and to provide other industries with compliance and inspection matters. The aim of the committee is to enhance maritime industry participation and awareness with matters related to ports and shipping security (DFT, 2008).

In 2007, The Department for Transport applied the National Maritime Security Program to cover domestic passenger shipping including tankers. The 2009 pre-arrival and pre-departure program of the European Commission also is a major mandatory European initiative to provide custom authorities with information about the imported and exported goods (Papa, 2013).I

4.2.5. Offshore Regulations

The UK governments' National Security Strategy realized the threat of international terrorism and its effect on its critical energy infrastructures. The Department of Energy and Climate Change has the responsibility for energy security and has established the overall approach to the protection and security of energy. Oil and Gas UK is the leading representative body for offshore oil and gas; in 2011, the Centre for Protection of National Infrastructures (CPNI) issued a security best practice guide for contracting staff in the oil and gas industry. The CPNI is the primary government authority that provides protection advice to the UK and it's essential facilities to counter terrorism and is inclusive of offshore oil and gas installations. The guidelines set some practical measures for personnel security that contracting staff should implement; these measures include risk assessments for personnel, access control, and cyber security (CPNI, 2011). One of the UK National Strategy for Maritime Security 2014 objectives includes measures for overseas territories and supports the security of offshore installations; while the Department for Transport is responsible for regulating merchant shipping, the Royal Navy is responsible for enforcing International Maritime Laws in ports and offshore installations.

4.2.6. Small Vessels Security

The DFT issued security guidance for maritime industries that are not regulated under the ISPS Code requirements (DFT, 2008). In 2011, the DFT issued such guidance for the Tidal River Thames Passenger Services (vessels and piers) to help increase passenger confidence in using river services and facilities, as well as to strengthen the overall maritime security within the UK. The guidance is a set of best practices and experiences gained through recommendations to enhance security by River Thames' vessels and operators. Although vessels that operate on River Thames are not covered by the ISPS framework, they should be aware of other ISPS vessels vesting the Thames as they may experience increased security measures at piers (Maritime Security Guidance Tidal River Thames Passenger Services, 2011). As part of the European Union, the UK implementation of EC 725/2004 Directive on enhancing ship and port facilities security allows it to deal with risks associated with small and non-SOLAS vessels by extending part A of the ISPS Code to cover passenger vessels in domestic trade shipping. Moreover, section 3 article 3 of the EC 725/2004 Directive, allows UK to decide the extent to which it will apply the provisions of this directive on different categories of ships operating in a domestic trade other than domestic passenger vessels, as mentioned in section 2 of article 3 of the EC 725/2004 Directive.

4.2.7. Marine Security Training

In order to appropriately manage UK port facilities in accordance with the ISPS Code, a port facility security officer is needed and is administered through the Ship and Port Facility Security Regulations (2004). Training courses must be completed and offered by training providers approved by and the Maritime Transport Security Division (MTSD)(a list of 31 approved training providers is provided by DFT via MTS) , as well as general security awareness training is required for staff carrying out other security functions at the port facility. The European Commission (EC) also imposes mandatory training for ships and port facilities' security officers in its regulation

275/2004. The DFT has dedicated teams of inspectors who are responsible for ensuring that all UK ports and ships are compliant with the ISPS Code; inspectors work closely with marine facilities' operators to ensure the effectiveness of security measures and plans. On the other hand, the Maritime and Coastguard Agency (MCA) inspectors are responsible for security compliance programs related to cargo and fright (i.e., the supply chain) (DFT, 2008).

4.3. United States of America

4.3.1. Overview

The Department of Homeland Security (DHS) is responsible to ensure that United States (US) national transportation systems and borders are secured. The U.S. shares 5,525 miles of borders with Canada and 1,989 miles with Mexico, as well as 95,000 miles of shoreline. There are nearly 350 official ports of entry in U.S. (Maritime Strategy for Homeland Security, 2002). The U.S. seaborne trade comprises 48% of the value and 78% of the weight of total U.S. imports and exports (HIS Global Insight, 2009). There are 3,200 cargo and passenger handling facilities that account for $212 billion of tax revenue in 2007, and offer about 13.2 billion employment opportunities (AAPA, U.S. Public Port Facts).

4.3.2. Regulatory Framework

The Maritime Transportation Security Act (*MTSA 2002)* was the first effort for the development of a systematic methodology for maritime security in the U.S. (Hardy, 2006). The *Act* contains 13 sections dealing with maritime transportation Security and requires maritime transportations to establish security plans as well as response teams to protect people and the marine industry. To enhance the overall security, section 70107 offers grants to maritime transportation to help in implementing security measures (MTSA, 2002).

4.3.2.1. The Security and Accountability for Every Port Act

The *Security and Accountability for Every Port Act (SAFE Port Act)* 2006 is one of the latest legislations for port and marine facilities security framework. By recognizing the importance of information sharing and operational monitoring with local port stakeholders, U.S. federal agencies have established inter-agency committees to improve the overall port and marine facilities security (Caldwell, 2007). There are some challenges and constrains associated with the implementation of the *SAFE Port Act* such as resource constraints, the speed and the scope of implementation, and container security implementation (Caldwell, 2007). However, the *SAFE Port* Act 2006 was established to adjust the existing security framework, which is mainly *MTSA 2002,* and to add more programs and initiatives. In short, the *Act's* main goals are to:

1. Codify the container security initiative (CSI), and the Customs-Trade Partnership Against Terrorism (C-TPAT), to reduce threats from container shipping;
2. Establish interagency operational centers to fit the security for ports;
3. Implement schedule and free restrictions for TWIC; and,
4. Implement containers radiation scanning and inspection (Caldwell, 2007).

4.3.3. Organizational Structure

The DHS is the lead federal agency responsible for the implantation of the *MTSA* requirements and regulations within the U.S. maritime security regime. However, the Maritime Administration under the National Shipping Authority can assume control over U.S. vessels and ports during emergencies (HIS Global Insight, 2009). In order for DHS to secure U.S. borders, the Department has incorporated the responsibilities of other agencies; for example, the U.S. Coast Guard (USCG) is the primary responsible agency for the U.S. maritime security domain and it leads the coordination of maritime information sharing and domain awareness. Part of USCG capacity is to conduct port facilities and vessels' inspections. The Transportation Security Administration (TSA)

responsibility is to control access of maritime personnel to marine and port facilities. To do so, Transportation Worker Identification Credential Program (TWICP) was implemented as a biometric (fingerprint template)[21] security credential that is issued for individuals who require access to marine facilities and vessels (Caldwell, 2012). The implementation of the TWICP was required by MTSA in section 70105 Transportation Security Cards. MTSA is also the primary responsible for allocating funds for port authorities and facility operators to implement security plans and to ensure the implementation of Areas of Maritime Security. The subsection 70107 of MTSA 2002 requires that TSA shall take into account national economic and strategic defense considerations when allocating security funds.

4.3.4. Major Initiatives

The U.S. Customs and Border Protection (CBP) are responsible for screening cargos and crew of all foreign vessels at ports of entry. CBP has initiated two important maritime security initiatives; the first is that the Container Security Initiative (CSI) is aimed to address threats to U.S. borders and global trade, which poses a vulnerability to security by which terrorist attacks can be delivered via container cargos (CSI, CBP). The second initiative is the Custom-Trade Partnership Against Terrorism (C-TPAT), which is a global supply chain security initiative made by CBP to extend the U.S. zone of security to the point of origin (C-TPAT, CBP). The Federal Emergency Management Agency (FEMA) is responsible for granting and administering funds for DHS to improve the security of U.S. for the marine and port facilities of highest risk (Caldwell, 2012). Section 70104 of MTSA requires the secretary of USCG to establish security incident response plans and to make

[21] Please refer to Caldwell Stephen L. 2012. Progress and Challenges 10 Years after the Maritime Transportation Security Act. U.S Government Accountability Office GAO-12-1009T. Retrieved from GAO on July 22, 2014 from: http://www.gao.gov/products/GAO-12-1009T

these plans available for the FEMA director for inclusion into the response plan for U.S. ports and waterways.

4.3.5. Offshore Regulations

According to the Bureau of Safety and Environment Enforcement (BSEE), there are 23 oil and gas platforms in the Pacific Region that account for 24 million barrels of oil and 47 million cubic feet of natural gas. The busiest offshore area in the U.S is the Mexican Gulf with an estimated 3,400 oil and gas platforms that account for 30% of the domestic oil and 11% of the domestic natural gas. The U.S.' legislations and regulations regarding oil and natural gas have been developed over decades. In the 1950s, the U.S. federal government began to increase its concern for offshore activities and jurisdiction. In 1953, states were given jurisdiction by *Submerged Lands Act* (SLA) over any natural resources within 3 nautical miles and the federal government were given the jurisdiction over submerged lands on the continental margin (Mastrangelo, 2005). Today, a number of U.S. federal government departments have jurisdiction over offshore oil and gas facilities and security, such as U.S. Coast Guard (USCG), Department of Transportation (DOT) and Department of Homeland Security (DHS). In terms of Offshore Mobile Drilling Units (OMDUs) and fixed oil and gas platforms that are not covered by ISPS Code, the security regulations set by USCG and DHS requires such installations and facilities to develop facility security plans and assessment reports, as well as to designate a security officer for the Outer Continental Shelf (OCS) facilities. The regulations also require offshore installations to implement security measures specific to the facility's operation, and to comply with all maritime security levels; however, for smaller personnel or production facilities, USCG must review the need for further security requirements. A set of standards could then be used, as separate rule-making would require compliance with industry standards of the American Petroleum Institute (API). The U.S. created the National Maritime Transportation Anti-Terrorism Plan to assess offshore energy infrastructures' vulnerability to

terrorism. The U.S. has improved offshore alert systems, intelligence, and integration by increasing the presence of the USCG and collaboration between regional and local regulators, military, and the Red Team (Northern Command's Anti-Terrorism) to assess offshore oil and gas industries (Avis, 2006).

4.3.6. Small Vessels Security

In 2012, the USCG estimated that there were more than 22 million small vessels (less than 300 gross tonnage) operating in the country. The DHS concluded that terrorists and other criminal organization could use such vessels for harmful activities since small vessels are considered unregulated maritime entities. This realization resulted in the conclusion that these vessels should be security regulated to reduce the vulnerability of the maritime security within the country and to create more consistent regulatory regimes for U.S. maritime security. As a result, DHS and its components (e.g., USCG and CBP) issued the Small Vessel Security Strategy and its implementation plan in 2008 to guide maritime industries to mitigate risks associated with small vessels. One of the key concerns voiced by USCG is that some large vessels (e.g., cruise ships) sail according to fixed schedules, which could provide information to terrorists in preparation for attacks against vessels and marine facilities. Moreover, these small vessels could be used for smuggling weapons into the country. The CBP and its Small Vessel Reporting System initiative concluded that the lower level of small vessels' compliant issues is due to lack of public awareness of the reporting requirements and lack of appropriate inspections. Another issue with small vessel security is that the IMO guidelines for the security of small vessels that are not subject to ISPS Code 2008 is a voluntary initiative, which makes it challenging for governments to implement and evaluate small vessel security (GAO report, 2013).

4.3.7. Marine Security Training

According to section 109 of the *Maritime Transportation Security Act 2002 (MTSA),* , the Secretary of Transportation is responsible for developing and implementing standards for maritime security personnel. In 2003, the joint Maritime Transportation and USCG Committee established a national system of maritime security personnel certification and course approval. The maritime administration (MARAD) prepared a report to congress to establish a voluntary program for maritime security personnel training and approval. This initiative is funded by the Maritime Administration/Coast Guard Joint Committee *MTSA 109* program on a fee-for-service basis (Maritime Administration Security Act Course Certification, MARAD).

- Based on the Guidelines for Maritime Security Training Course Providers, the Maritime Administration (MARAD),the USCG, and the National Maritime Centre (NMC) have the authority to assess and approve maritime security training course providers; currently, there are more than 50 certified maritime security training providers that have been approved by Det Norske Veritas (DNV), a USCG -accepted organization. Training providers are required to pay 75% of the processing fees to MARAD. They also have to be eligible and authorized to conduct business under the federal and the states laws. The MARAD provides a list of guidelines, model courses, competence tables and certified course institutions to help service providers enhance maritime security on national and international levels. Maritime security service providers are mainly offering 6 training course, which include:Company Security Officer (CSO) and Facility Security Officer (FSO).
- Maritime Security for Vessel and Facility Personnel with Specific Security Duties (VPSSD and FPSSD).
- Maritime Security Awareness (MSA).

- Maritime Security for Military, First Responder, and Law Enforcement Personnel (MSLEP).

4.4. Canada

4.4.1. Overview

As a marine nation , Canada has approximately 243,000 km of coastline, the longest in the world with access to the Atlantic, Pacific, and Arctic oceans (TC, 2011)[22]. In 2010, the Canadian maritime trade industry was worth $170 billion andthere were about 324 ports and harbors within Canada that handled about 302 million metric tons of international trade in 2009. The annual economic trade of Canada's ocean is worth about $100 billion and the Canadian ports industry is offering more than 250,000 jobs. There are 18 distinct Canadian Port Authorities (CPAs) that are financially self-efficient and account for 58% of the international trade, 36.4% of the domestic trade, and 100% of the container traffic in 2003 (AAPA, Canadian Port Industry).

4.4.2. Regulatory Framework

Transport Canada (TC) leads the government's initiatives in marine security with the role and responsibility to develop marine security regulations and initiatives, as well as to manage the security enforcement and compliance within Canada's maritime security regime[23]. TC is also responsible for coordinating policy, chairing the interdepartmental Marine security-working group (IMSWG), and managing Marine Transportation security clearance program and participating in the marine security operation centers (TC, 2011).

[22]Please refer to Transport Canada Marine Safety Publications-TP 14916 E (2011). Canada: committed to the goals of international maritime Community. This publication gives an overview and some statistics about Canada marine industry. http://www.tc.gc.ca/eng/marinesafety/tp-tp14916-menu-182.htm

[23] Please refer to Transport Canada 2014-15 report on plans and priorities, Horizontal initiatives at http://www.tc.gc.ca/eng/corporate-services/planning-rpp-2014-2015-1111.html

The Canadian framework for security measures of marine vessels and port facilities came into force as the *Marine Transportation Security Act* (MTSA) 2004 and Marine Transport Security Regulations (MTSR) were designed to address Canada's obligations to implement the ISPS Code. The *MTSA* gives the Minister of Transportation the authority to regulate and take the necessary security measures to protect and reduce security gaps of Canada's marine transportation industry. The MTSR established the responsibilities for developing security plans and provides a guidance to conduct security assessments and protocols for marine facilities, ports, and vessels (TC, 2004). The *MTSA* and MTSR are the foundation for rules regarding securing marine transportations against unlawful interference.

4.4.3. Organizational Structure

The marine security regime in Canada is a complex and a multi-faceted activity that needs to be periodically reviewed with partners and stakeholders to address new and evolving threats to the security environment. It is also horizontally-initiated to improve the security of Canada's marine domain and includes waterways, land, and ports (TC, 2011)[24]. The marine security has been a consistent part of the Canadian transportation system since the 1994 legislation of the *Marine Transportation Security Act* (Kinney, 2009).

There are several government department, agencies, and authorities that have a role to play in Canada's marine security. The Department of National Defense (DND) is the lead department of the overall coordination of on-the-water response to security threats. Its responsibility of security response covers all coastal areas up to the EEZ limits. Besides its response to security threats and crisis, DND assists other departments (e.g., Department of Fisheries and Oceans Canada, Department of Environment) in their protection, disaster relief, and search and rescue services (Kinney, 2009).

[24] Please refer to Transport Canada 2014-15 report on plans and priorities, Horizontal initiatives at http://www.tc.gc.ca/eng/corporate-services/planning-rpp-2014-2015-1111.html

The Canadian Coast Guard (CCG) is involved in marine security based on its obligation under the *Oceans Act* and it is part of the Department of Fishers and Ocean (DFO). CCG uses its fleets and capabilities to enhance awareness of possible marine security threats by using the Automatic Identification System (AIS) to monitor vessel tracking. The CCG also supports on-the-water enforcement and responses as they are the operator of Canada's federal civilian fleet. Moreover, the multi-agency approach of Canada's marine security gives the CCG Maritime Security Branch the responsibility for working with partners to develop and implement Canadian Marine Security Strategies (CCG, Maritime Security).

The primary role of the Royal Canadian Mounted Police (RCMP) is to investigate national marine security threats , although it has other enforcement mandates on diverse security matters and other operational support services for policing (Kinney, 2009). There is also the Canada Border Services Agency (CBSA), which manages Canadian borders and enforces international agreements, domestic trade and travel regulations. The mandate of CBSA authorizes the agency to seize goods, make arrests, and investigate matters related to marine and border security. The CBSA was established in 2003 as an integral part of the public safety, which aims to protect Canadian society, and therefore has the responsibility to support national security and public safety endeavors and to ensure the free flow of goods and people to and from Canada. According to CBSA Audit of Border Controls for Marine Ports of Entry (Final Report, December 2012), over 95% of marine cargo was imported into Canada through five major ports (including Halifax) with over 2.5 million containers imported into Canada in 2011. The marine program identifies inadmissible people and goods, and ensures legitimacy within service standards for travelers and commercial streams at the marine port of entry. While the Integrated Primary Inspection Line Program is used to process passengers at the terminal, Cargo Inspection Systems (e.g., scanning technologies) are used to process the flow of

goods in the commercial stream of the supply chain (CBSA). The security of marine ports and facilities is a shared responsibility between the agency, TC, port authorities, and the operator.

In spite of the fact that CBSA does not have 24-hour inspection at ports, marine terminal operators have the mandate and obligation under the Customs Sufferance Warehouse Regulations to provide security duties for goods at all times. The CBSA also relies on marine facilities' operators for the implementing radiation detection regimes at major ports, as are other security measures (e.g., adequate fencing and access control) as required by TC marine security implementation programs (CBSA Final Report, 2012). Lastly, the Canadian Security Intelligence Service (CSIS) provides the federal government with the capacity to investigate security information and anything that could threaten Canadian security in conjunction with other departments such as the Department of Public Safety Canada, RCMP, and CBSA for policing and enforcement matters (Kinney, 2009).

4.4.4. Major Initiatives

4.4.4.1. Interdepartmental Marine Security Working Group

The *Interdepartmental Marine Security Working Group* (IMSWG) was created in 2001 as a forum whereby several federal-level government members can identify and coordinate national initiatives to enhance Canada's marine security regimes. The IMSWG involves 17 federal departments and agencies that work harmoniously to develop policy recommendations for decision makers and promote the collaboration and communication efforts across different levels of government (NSF Consultants, 2004). The IMSWG meets at a minimum of 4 times a year to coordinate marine security policy; however, the IMSWG sub-committees (e.g., policy, operation and legal committees) meet monthly in order to address and provide guidance on contemporary policies, legislative gaps, and regulatory issues to best advance marine security priorities (TC, IMSWG).

4.4.4.2. Marine Transport Security Clearance Program

The Marine Transportation Security Clearance Program (MTSCP) has been implemented through Canada's Airports Security Initiatives since 1985. In 2003, the MTSCP was expanded to cover the Marine Transportation Security. TC initiated the MTSCP in 2003 in response to an ISPS Code that required measures to reduce the risk of security threats resulting from employees and people interacting with different marine transportation systems. The main purpose of MTSCP is to conduct a background checks on marine employees who have access to restricted areas within ports and marine facilities. In 2009, TC and the RCMP signed an agreement to share law enforcement information to enable the MTSCP's decision-making to be based on more complete data from different intelligence sources (TC, Comprehensive review, 2011). Based on a global evaluation of the information obtained regarding the employee, the TC Intelligent Branch can decide whether to grant a security clearance to the applicant (TC, MTSCP).

4.4.4.3. Marine Security Operation Centers

The Marine Security Operation Centers (MSOCs) were established in 2004 by the National Security Policy to enhance marine security for Canada and its allies. There are three operational centers; the RCMP operates one and the Department of National Defense (DND) leads the other two. These centers are built on a multi-agency integration approach, which includes TC, DND, RCMP, DFO, CBSA, and the CCG. Each department maintains its mandate and role, and communicates with the other agencies via information systems and expertise exchange (CCG, MSOC).

4.4.5. Offshore Regulations

On January 30th, 2014, the Canadian Minister of Natural Resources introduced the *Energy Safety and Security Act.* The new Act will help provinces to introduce new legislative instrumentations and amend the existing *Accords Act* liability provisions, as well as to enable

operators to post more security requirements and environment liability. This latter step will enable provinces with offshore oil and gas industries to strengthen legislation and provide greater economic benefits by ensuring the security of the offshore industry (Andrew Younger, NS Energy Minister, 2014). The existing *MTSA* and its regulations authorize TC to regulate the security regimes of offshore oil and gas facilities, such as Mobile Offshore Installations (MOIs) and the vessels serving them (TC, Security of Offshore Installations, 2010). However, some of the offshore oil and gas installations (e.g., fixed and non-self-propelled offshore platforms) remain beyond the scope of national and international legislations.

For example, the Canada-Nova Scotia Offshore Petroleum Board (CNSOPB) continues to manage its security regimes based on the API 70 (1) best practice for security on offshore installation. Dissimilarly, the Canada-Newfoundland and Labrador Offshore Petroleum Board uses a different approach whereby it adopted ISPS Code security measures. In spite of the efforts of the DND in protecting the maritime regime by establishing the Joint Task Force Two to counter terrorism within offshore areas there are still some capacity and training challenges that need to be standardized and/or mitigated (Avis, 2006).

4.4.6. Small Vessels Security

The voluntary initiative MSC.1/Circ.1283 made by IMO was introduced in 2008. It's aim is to help maritime security authorities in establishing plans for security incidents, promoting security awareness, and preventing unlawful acts; the latter includes unauthorized access to small vessels such as small fishing vessels, pleasure crafts, passenger vessels, and commercial non-passenger and special purpose vessels (IMO, MSC.1/Circ.1283, 2008). TC has taken the approach of promoting security awareness to keep small vessel and small facilities safe and secure. In spite the fact that small vessels security is the responsibility of the owner, reporting of suspicious activities should be

made to the RCMP and the provincial and municipal police authorities (TC, small fishing vessel security awareness, 2010).

Although *MTSA* does not apply to the domestic ferry industry, TC has initiated Domestic Ferries Security Regulations framework to enhance Canadian ferry security and promote trade competition. The step currently applies to approximately 50 ferries operators on 18 routes to 29 ferry facilities within Canada (DFSR, TC).

4.4.7. Marine Security Training

Transport Canada is obligated by the ISPS Code to ensure that appropriate training is made available; a number of commercial institutions are approved to provide ISPS Code training courses. The Transport Canada Recognition Program for Marine Security Training Programs and Courses is a voluntary program established in April 2003 to ensure that marine security training and courses for marine officers meets the requirement of ISPS code and MTSRs (TC Recognition Program for Marine Security Training Programs/ Courses, 2007). The director of Marine Security Operations is responsible for reviewing and verifying the course content while the training provider is responsible to deliver security training based on IMO model courses and MTSR duties for security officers. Currently, TC is in the process of amending MTSR so as to meet the new requirements and implementation strategies of the new Manila 2010 STCW which came into effect in January 2012 (Marine Security Operations Bulletin 003, 2013).

5. Results

5.1. Differences in Initiatives and Frameworks

In order to implement new regulatory frameworks, contracting counties have taken different approaches. The result of the urgency to implement the ISPS Code has created an incoherent integrated approach (Papa, 2013). For example, the ISPS Code excludes small vessels such as vessels less than 500 gross tonnage from its scope, thus creating a gap in the marine security regime. Moreover, ILO and IMO codes of practice for the security in ports provide a common approach for contacting governments to follow. While Australian authorities consider it an offence for non-compliant marine facilities to operate without assessing their security, Canadian regulations conditionally allow marine facilities to operate as an occasional-use marine facility. The issue, however, with occasional-use marine facilities is that they do not require security assessments and plans to be in place. Moreover, the proposed amendments to MTSR in 2013 provide the domestic shipping sector the flexibility and choice to interact with unregulated marine facilities based on their business needs. Additionally, this approach would increase the costs associated with greater security procedures for the vessels' security plans; unregulated marine facility security has not yet been properly managed, and is still considered a threat to Canada's maritime security regime.

UNCTAD has promoted that effective compliance measurements for maritime actors are difficult to undertake on a global scale due to the sheer number of sectors involved in the maritime industry, as well as the different approaches taken by contracting governments to manage compliance with the SOLAS measures (UNCTAD, 2006); the maritime security measures are classified as following;

1. International standards programs
2. Government programs
3. Customs compliance programs

4. Private sector programs

In an attempt to balance between security and trade, the Australian government has implemented its regulations through the Department of Infrastructure; Border Protection Command (BCP) has the lead authority when encountering terrorism threats. Encountering maritime threats require sufficient capacities and enforcement authorities such as the Australian BCP. This factor may have helped Australia to balance its trade objectives with maritime security protection regimes. Trade oriented approaches have been adopted by the U.K. and Canada by giving the lead to Department of Transportation. In contrast, the U.S. government took a more secure approach by giving the lead to Homeland Security department.

Two marine security programs have influenced the development of marine security regulations within Canada. The IMO provided Canadian governments with security standards for the ships and ports serving them. The result was that Canada's marine transportation security regulations have incorporated them into section 5 of Canada's *Marine Transportation Act* (1994). Given that U.S. is the primary trade partner with Canada, it is important for Canada to complement U.S. marine security regime (Ircha, 2011), and work extensively with U.S. to facilitate security and trade efficiencies. According to Ircha (2011), half of the containers handled in the Port of Montreal are either going to or coming from the U.S., and nearly 100% of the containers in Prince Rupert container terminal are shipped to the U.S. Furthermore, the Canadian-U.S. Regulatory Cooperation Council (RCC) is working on aligning Canada's regulatory approaches to eliminate duplication and impediments to better facilitate trade between Canada and U.S without comprising security. For instance, Canada is proposing a new schedule to its regulations so as to expand the list of certain dangerous goods that the vessels could carry in order to align them with the U.S. list (Regulatory Impact Analysis Statement, 2013). The complementary approach adopted by Canada to match that of the U.S. marine security programs is creating a balance between security and trade regulations.

5.2. Misinterpretations of the ISPS Code have created Regulatory Challenges

The national approaches taken by contracting government for maritime security regime have faced many challenges. The IMO deadline for implementing ISPS Code by July 2004 has led contracting government to establish their national security standards and incorporate ISPS Code within these regulations. In Canada, the Canadian Association of Port Authorities has addressed some of the challenges and regulatory gaps respecting to the port and marine facilities implementation of the new regulations. In Sep 28, 2003, CPAs and marine facilities operators have submitted a report to TC on the proposed marine transportation security regulations. Five key issues were identified by ACAP. First, TC has given CPAs and marine facility operators a role in implementing ISPS Code and submitting security plans without defining the liability[25]. Second, there was no clear enforcement regime for non-compliance marine facility operators because the enforcement regime was built on a voluntary implementation. This matter is important because it may result in black listing of the marine facility and the port by IMO. Third, there was no clear vision for the authority responsible for waterside security. This issue is also important for the port security system, which requires resources, capacity and new initiative (ACPA, 2004). Australian approach to waterside security is clearly defined in its regulations under section 6.70, which requires that port operators must ensure access to waterside restricted zones and take the necessary measures to control and detect access to those areas (MTOFSR, 2005). Fifth, processing time and funding of implementing ISPS Code requirements is needed to be harmonized with neighbors in order to achieve security enhancements and trade competition particularly with USA ports (ACPA, 2004). However, the proposed amendments of 2013 to MTSRs has addressed the Government of Canada's Red Tap Reduction Commission recommendations by reducing financial and regulatory

[25] Please refer to Association of Canadian Port Authorities .2004.Submission to Transport Canada on Proposed Marine Transport Security Regulations. Retrieved From: www.acpa-ports.net/advocacy/pdfs/formal_submission04.pd

burden, and by harmonizing some regulations such as Certain Dangerous Cargoes (CDC) expanding list regulations with U.S marine security regime (TC Regulatory Impact Analysis Statement, 2013).

To conclude, it can be said that Canada marine security strategy is trade oriented which can be seen in the proposed amendment to MTSR OF April 27 2013. However, to facilitate trade and increase economic benefits, there are still some regulatory gaps that need to be properly reduced. One of which is a non-SOLAS ship security and unregulated marine facilities. To properly address security threats and mitigate risks, security plans and assessment are needed for ports and marine facilities. The location and important infrastructure within the port area need to be well protected by security plans when port authority and marine facility operator submit their application to approve their security plans to the Minister.

In the case of Richmond terminal, would require a full compliant statement because of the following reasons;

1. The area of the terminal is huge when comparing it with other facilities and is located in one of the major ports of Canada.

2. Close proximity and location to many critical infrastructures, MacKay Bridge, Highway, Navy base, as well as the narrow navigable water to Bedford Basin.

3. A variety of users will be utilizing the terminal because it is a mixed-use marine facility. There will be different marine users (regulated and unregulated) utilizing the terminal, which needs a clear set of security regulations in place to avoid conflict.

4. Marketing the terminal as a fully compliant marine facility will attract stakeholders and promote national and international trade.

5.3. Supply chain security initiatives focus on specific marine industry (container).

Most of the maritime security initiatives for ports and marine facilities have dealt with border and custom aspects of securing maritime ports. UK has implemented the Pre-arrival and Pre-departure program of the European Commission 2009 to reduce potential imported and exported containerized goods threat at ports and their facilities. Similarly, the U.S Custom and Border Protection initiative for Container Security (CSI) was introduced in 2002 to protect global maritime trade from interruption and enhance efficiency of the supply chain. Giving that U.S is the main trade partner to Canada with an average of 4.5 yearly increase (Hansen, 2011), the Canadian Border Service Agency has signed in 2005 a partnership arrangement with U.S Customs and Border Protection Department to promote not only the land-based trade between Canada and U.S but also international maritime security and trade. The Atlantic Gateway Strategy aims to improve Canada's global trade. It is expected that the volume of Maritime trade in the Atlantic Region will increase and its importance to security will also increase (Hansen, 2011). The issue with CSI and other international screening and detection initiatives of containers however is that many counties has not implemented such initiatives which still imposes potential threats to maritime trade security. Moreover, CSI is targeting major ports, which leaves small ports and marine facilities out of the scope of CSI. CBSA for example does not work in each marine facility and does not have a 24 hours service in each port of entry (Container Security Initiative in summary, US Customs and Border Protection, 2011). A great attention has been paid to container and passenger security while not much attention has been paid to general cargo security (Baker, 2007). General cargo vessels may be used as a weapon to attack coastal infrastructures.

5.4. Critical marine industry omitted from national and international legislations

The world's largest marine industry is offshore oil and gas. Attacks on offshore oil and gas installation could have not only interruption of the energy supply but also damage to the

environment. Much of the government's marine transportation policy focused on vessels, marine facilities and ports security. Moreover, UNCLOS 1982 has giving coastal states a broad jurisdiction to protect offshore assets within territorial and contiguous zone but fewer rights within the EEZ, except establishment of a 500-meter safety zone (Williams, 2013). This has left offshore installations more vulnerable to threats (Harel, 2012). According to the Council for Security Cooperation in the Asia Pacific Memorandum NO.16 for the safety and security of offshore oil and gas installations, there is a number of emerging issues and potential consequences for the increased offshore oil and gas activities. To name few, Increase in maritime traffic will increase the likelihood of oil environment damage and terrorist attacks as well as the likelihood increase of unregulated and unauthorized activities. Threats to offshore industry may also result from inconsistent and uneven adoption and implementation to the maritime security regime in many regions in the world. For instance, in Canada, Newfoundland and Labrador Offshore Petroleum Board has implemented ISPS Code and MTSR in its security demands but the Nova Scotia Offshore Petroleum Board has not taken such an action yet, and it is still uses the API security practices in its operations. This is clearly to be seen from the different approaches taken contracting governments to secure their maritime regime. Increase insurance and law initiatives may affect the cooperation arrangement financing consequences (e.g. piracy and armed robbery) (CSCAP, 2011). While some counties such as Australia took the approach of integrate energy protection in its marine security initiatives, Canada's jurisdiction over the energy security is still a shared responsibility between different levels of governance. These shared responsibilities over the energy sector impose challenge to regulate offshore oil and gas industry. The existing regulations and national security policies of Canada's offshore oil and gas security are out of date and incomplete (Accords Acts), to offer the protection for offshore energy installations (Avis, 2006). The focus of the Accords Acts was mainly

on safety and environment protection and the Canadian Critical Infrastructure Protection Strategy excluded offshore installations from its scope (Avis, 2006).

5.5. Unbalanced trade and security requirements.

"In order to benefit from efficient and effective global supply chain, the security-related activities incurred must be completely synchronized with the requirement of the said global supply chain management. Security initiatives are now being considered part of the key logistical activities but it is at the same time one of the most problematic activities, especially in an international context. If the security activity fails to perform, this will surely impact on competiveness of global supply chain" (Banomyong, 2005).

According to Transport Canada Maritime Commerce Resilience Planning Program (MCR), the global maritime transportation system moves over 90 % of the world's trade. Any major or long-term disruption would have severe impact on Canada and the global economy. TC to help Canada's global competitiveness as a strong trade partner established the Canadian MCR planning initiative. The MCR help Canada maritime trade by ensuring the continuity of maritime commerce, awareness of emergency and communication process and the recovery of the maritime operations after disruptive events (TC, MCR). The EC Directive 65/2005 on enhancing port security states that "people, infrastructure and equipment in ports should be protected against security incidents and their devastating effect. Such protection would benefit transport users, the economy and society as a whole".

It is crucial for international trade to have efficient, adaptable and integrated transportation systems to ensure the business continuity. A range of security and trade measures must be taken by private sectors and public players to maximize the benefits of international trade. The strategy of Atlantic Gateway and Trade Corridors for infrastructure investment requires that stakeholders must be built on competitiveness on national and international trade. Transportation systems also are

encouraged to improve national and international operational standards (Atlantic Gateway, TC Strategy). The strategy of Atlantic Gateway and Trade Corridors for infrastructure enhancement requires public and private sector to have knowledge of system impediments. For the case of Richmond Terminal at the port of Halifax, security requirements is one of these impediments that need to be properly managed to achieve the goals of Atlantic Gateway and Trade Corridors ultimate goal of maximizing national and international trade and support economic opportunities. In 2004, A report prepared by CFN Consultants states that, "there is an economic incentive to promote the safety and security reputation of Canadian port facilities because perception in trade has as great an effect on the preferred routes for the movement of cargo as physical reality, there are competitive reasons for establishing a highly visible port security profile' (page, 10). Thus, to facilitate international trade competiveness, Canada has to continue respond to international obligations and align or harmonize its regulations with international partners. For example, Canada is required to implement the new amendments to STCW. National obligations also need to be reviewed and aligned with the existing regulations in order to reduce the regulatory and financial burden (TC Regulatory Impact Analysis Statement, April 27, 2013). Recently, the Beyond Action Plan for Perimeter Security and Economic Competiveness was initiated between Canada and the U.S to facilitate stakeholders and government departments trade flow in secure and competitiveness environment[26]. Realizing the important of communication and information sharing, TC connects coastal marine security centers to the government of Canada's most secure communication and intelligence network. Phone calls as well are now routed for better efficiency of operation and services. Furthermore, the Marine Event Response and the Maritime Operational Threat Response Strategic Protocol was established in 2012 between Canada and the U.S, to facilitate information sharing during security threat events (Transportation in Canada 2012, Overview Report). Another

[26] please refer to Perimeter Security and Economic Competitiveness Action Plan(2011). Retrieved on 22 July, 2014 from: http://actionplan.gc.ca/en/page/bbg-tpf/beyond-border-action-plan-brief

aspect that should mentioned here is the issue of funding marine security. The UNCTAD analytical framework for compliance measurement and risk assessment for maritime security has divided financing approaches taken by states as following;

1. Operators pay the cost of regulations, which is been used in UK and Canada.
2. Public Authorities pay the all cost, Canada.
3. Parties shared cost, which is the approach adopted by the U.S. where all public and private sector share the cost of the regulations (UNCTAD, 2006).

Within Canada, there have been significant amount of funding made to enhance marine security. For instance, a $115 million federal budget was allocated in 2004 to enhance port security by improving security fences, communication devices, and surveillance. Although, there were no clear summary of the government expenses on how the funds are being distributed on security programs and industrial opportunities (CFN Consultants, 2004). In spite of the number of initiatives and regulation taken by TC and the federal government to enhance port security and trade, there is still a need for more funds to support additional port facilities security initiatives. The American Association of Port Authorities realizes that one of the major U.S. ports' issues is expanding source for seaport development financing and revenue, including for seaport security measures. Additional funds and security initiatives programs should be targeting promoting Canadian ports security to be able to compete with major trade partners of Canada (Ircha, 2011).

A comprehensive research by Public Policy Institute of California (PPIC) on balancing security and cost of the national seaports has found that the economic effects of a terrorist attack a port could be severe and have direct and indirect consequences. In a one-year reconstruction scenario, a terrorist attack of the four connected the mainland with the Terminal Island of the port of Los Angeles; the U.S economy could lose $45 billion, 280,000 jobs (Haveman, &Shatz, 2006). On the

other hand, the benefits of preventing a terrorist attack at a Canadian port could range between $20 million to $57 billion (Regulatory Impact Analysis Statement, 2013).

5.6. A Balanced Approach in Australia

The Australian model for maritime industry security is a balanced approach between trade and security requirements. While the office of transportation is a key principle for the management of maritime security, the Border Protection Command is the lead agency when encountering terrorism threats. Incorporating offshore facilities into the national maritime security framework (i.e., MTOSR) in 2005 has enhanced and improved the consistency of the overall maritime security regime. The early implementation of the newly amended framework has also helped maritime industry to adapt their security requirements while simultaneously trading. For unregulated marine facilities, a security guideline was issued in 2014 by the Department of Infrastructure and Regional Development, which requires such facilities to perform security assessments and implement the appropriate security procedures to mitigate the potential threats. Like Canada, Australian offshore oil and gas installations are located in far from shore, which requires fast responses and early warning signs to effectively manage. The establishment of the Taskforce on Offshore Maritime Security in 2004 as a central body of Australia's counter-terrorism and provides offshore installations with the necessary patrol and surveillance capacities. In terms of border protection, the Australian Maritime Security Operation Centre (AMSOC) has integrated officers from different agencies such as safety and fishing for an interdisciplinary management approach. The AMSOC is also responsible for implementing AMIS to facilitate information sharing about maritime security threats regularly for 24 hours a day. The Australian Border Protection Command uses an intelligence-led risk-based intervention approach to protect the border in the trade environment. Amendments to the *Customs Act* in 2013 place statuary obligations on cargo terminal operators, including mandatory reporting of unlawful activities and ensuring the physical security of cargo.

5.7. International Weaknesses for Oil and Gas Installations and other maritime participants Security

The weaknesses within the different security regimes regarding offshore oil and gas installations and non-compliant marine industries could be summarized as the following two topics.

First is the lack of regulatory frameworks for the security of offshore installations and non-compliant marine entities. In 2011, U.K. had issued security guidelines of best practices for personnel working on offshore installations. However, rather than focusing on the best practices and procedures, nations should instead design clear security guidelines that are based on risk assessments and plans for the sustainable security of offshore installations. In spite the fact that section B of the ISPS code (the recommended guidelines) has been made a mandatory measure by the European Commission regulations, offshore installations are still not covered under E.U. regulations. The U.S. offshore oil and gas security is extensive and includes a number of regulatory agencies. However, the huge number of offshore oil and gas industries, especially in the Gulf of Mexico, encompasses approximately 3,400 installations; close proximity of these installations imposes threats and vulnerability that require greater capacities and funds to address.

Transport Canada has excluded fixed and non-propelled offshore oil and gas installations from its regulatory security framework. Based on the requirements of Canada-Newfoundland and Labrador Offshore Petroleum Board, installations along the Newfoundland and Labrador continental shelf are fairly well protected by having adopted the ISPS code requirements. However, the security of installations within the Nova Scotian continental shelf may yet still be managed based upon the security best practices of the American Petroleum Institute (API). This issue highlights the regulatory gaps existing within the Canadian Regulatory framework for security of maritime industry. Yet, allowing offshore supply vessels to interact with unregulated offshore marine facility and port marine facilities in the supply chain cycle would widen the gap and

increase vulnerabilities of the whole maritime security regime. Moreover, small and non-SOLAS vessels (e.g., those used for a domestic trading fishing vessels) that interact with marine facilities are not seriously managed; promoting security awareness should be enforced at minimum.

Second, there has been great attention being paid to container security and vessel passengers. However, cargo ships' security regimes, such as customs and border protection security, have not been properly managed. For example, the Canada Border Services Agency (CBSA) does not have 24-hours inspection at ports and marine terminals. Operators have the mandate and obligation under the Customs Sufferance Warehouse Regulations to provide security duties for goods. While the CBSA relies on marine facilities' operators for implementing radiation detection regimes at major ports, select security measures (e.g., perimeter fencing and access control) are required by TC marine security implementation programs. This example exemplifies the potential jurisdictional overlaps between operators and TC vessels simultaneously utilizing a marine facility[27]. Moreover, the U.S. CSI and C-TPAT provides security for containers' goods, though they are costly to implement, and targeting only major ports.

5.8. Results Summary and Consequences of OUMFs

In summary, a number of issues need to be resolved before establishing a proper regulatory framework for the security of mixed-use marine facilities and ports facilities in general. First, the security of small vessels and non-compliant marine industries, such as fixed and non-propelled offshore oil and gas, should be comprehensively assessed during the planning stage and vigorously discussed with stakeholders. Second, given that a number of vessels and users will be simultaneously utilizing a port facility, there is a need to consider any regulatory overlaps between different jurisdictional bodies, including border protection and port authorities.

[27] Please refer to Canada Border Services Agency Audit of Border Controls For Marine Ports of Entry, Final Report December 2012. Retrieved on July 23, 2014 from: www.cbsa.asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2012/auditbcmarinepoe-verifcfpemaritimes-eng.html#a1

The results from the four international case study analyses are summarized below in Table 1. Five negative characteristics to avoid in order to achieve a viable marine security approach and must be prevented at the planning stage for marine port and facility security regimes at Richmond Terminal and Sheet Harbor are summarized as the following:

1. Incoherently integrated approaches have been adopted only to satisfy international standards.
2. Common misinterpretations of the ISPS code security measures that have created challenges and regulatory gaps.
3. Supply chain security initiatives focus primarily on specific marine industry (e.g., containers).
4. Huge marine industry has been exempted from the scope of national and international legislations (e.g., offshore sector).
5. Imbalance between trade and security requirements and interests.

Table 1. Summary of the four international examples (i.e., Australia, Canada, United Kingdom [UK], and United States [US]) of maritime security regimes according to their frameworks, authorities, initiatives, orientation, and training.

	Australia	**Canada**	**United Kingdom**	**United States**
Framework	Maritime Transport and Offshore Security Regulations 2005	Marine Transportation Security Regulations 2003	Port security regulations 2009+	Marine Transportation Security Regulations 2002; The Security and Accountability for Every Port Act 2006
Authority	Office of Transport Security; Department of Infrastructure and regional development	Transportation Canada	Department for Transport	Department of Homeland Security
Initiatives	Maritime Security Operation Centre; Maritime Security Identification Card	Maritime Transport Security Clearance Program; Marine Security Operation Centers	The National Maritime Committee	Container Security Initiative; Transportation Worker Identification Program; Custom-Trade Partnership Against Terrorism
Orientation	Trade: Multi-Agency	Trade: Horizontal – Multi-Agency	Trade: Multi-agency	Security
Training	AMSA Responsibility	TC Recognition Program Responsibility	MTSD Responsibility	MARAD Responsibility

The significance of this table is to demonstrate that the authority responsible for implementing maritime security frameworks plays a major role in shaping the country towards marine industry orientations. Canada, Australia, and UK gave transportation departments the responsibility to implement maritime security regulations. They also adopted multi-agency approaches to manage their maritime security regimes. This may have created some challenges for these nations to balance trade with security requirements in terms implementing new security requirements. In contrast, the U.S. established the Department of Homeland Security to manage its maritime security regime. This may has created some challenges for U.S. in terms of adding more

cost for marine participant to meet the security requirements and degrading trade facilitation. Ultimately, there is a trade-off between having either a trade- or security-based regime that dominates the flow of operations and flavor of regulations and legislation. In either case, it is important for nations to better balance their approaches to maritime trade and security so as to not disadvantage the other.

6. Discussion and Analysis

6.1. Richmond Terminal

The common problems within the Canadian Maritime Security regime with regard to marine facilities and ports security could be summarized as the following;

1. Regulatory gaps in offshore oil and gas sectors' security implementation and strategies.
2. Regulatory gaps in small vessels' security implementation and strategies.
3. Regulatory overlaps between border protection and marine facilities security management agencies.

The OUMF approach has only been implemented within the context of the Canadian Maritime Security Regulatory Framework. The advantages of OUMF's regulations include addressing the security of small rural marine facilities and reduce costs associated with implementing security measures for marine industries. They also offer a transitional stage for port authorities and operators to be prepared for a fully-compliant marine facility exceeds 10 vessel-facility interactions annually. However, OUMFs are not required to perform risk assessments nor develop a comprehensive plan. Thus, establishing a OUMF within a major port, such as the Port of Halifax, represents vulnerability to the port's infrastructure. The protection of the critical infrastructure adjacent to the Richmond Terminal (i.e., bridges, navy base, communication facilities, and narrow navigable waters) would not be properly assessed since existing OUMFs would not have prioritized or assessed these structures for risk. Besides the flexibility OUMFs offer to port authorities (e.g., cost reduction, and interacting trends), OUMFs should not be established within major ports. Unlike Sheet Harbor Terminal, Richmond Terminal is located adjacent to critical infrastructure in the Port of Halifax, covers a greater area, and serves many multi-use operators. Moreover, OUMFs are vulnerable to security threats. The Richmond Terminal is a mixed-use marine facility that can be simultaneously

utilized by many operators, and so a number of non-compliant marine facilities may also simultaneously interact with the terminal.

The supply chains' security regimes for offshore oil and gas industries in Canada are not properly managed. The two most common weak links that exist within the supply chain are the OUMFs, fixed and non-self-propelled offshore oil and gas installations. To address this, Australia has already incorporated the offshore installations within its regulatory framework. Besides its capacities to protect its marine offshore industry, U.S. DHS requires offshore installations to assess their risk based upon the international standards. There is a lack of clear and consistent regulatory frameworks for the security of such an installations in Canada. Thus, allowing any interaction between fully compliant marine facilities (including OUMFs) and non-compliance offshore oil and gas installations represented a regulatory gap in the maritime security regime in Canada that needs to be addressed.

Given that the CBSA does not have inspectors at all Canadian marine facilities, there is a possibility that regulatory overlaps could exist among the authorities responsible for the security of cargos and goods. As a mixed-use marine facility, Richmond Terminal can handle a variety of cargoes such as containers, CDC, and special projects cargoes. The international framework did not properly address the security of general cargoes. In many cases, CBSA will delegate the responsibility of inspection to the operators, although they do not possess the legislative authority.

The security strategy of the Atlantic Gateway and Trade Corridors (AGTC) is to facilitate trade and enhance supply chain competition. The incentive of AGTC to promote safety and security profiles for ports is largely a result of trade competition that requires a high level of port security measures. Because Richmond Terminal has an OUMF and thus does not have a suitable security plan in place it cannot promote international trade. On the other hand, the number of trade

competitions and vessels' interactions with ocean terminals are increasing due to security measures (such as vascular screening technology) in place.

6.2. International trends in maritime security

The national AGTC strategy was designed to enhance and facilitate trade within an integrated security environment, in accordance with international standards. Recently, the international trend is building towards establishing new initiatives that have the ability to meet the increased trade in the domestic and international marine transportation systems. For instance, U.S. DHS had issued new security regulations to address small and domestic vessels security in 2008; this U.S. strategy is intended for domestic security purposes. In 2009, the U.K. had implemented their port security regulations by integrating ISPS Code and the EC Directive 725/2004 into the local measures[28]. A voluntary guideline for small vessels and facilities was drafted by IMO in 2008. Transport Canada helped IMO in drafting specific recommendation guidelines for small vessels security[29].

6.2.1. Lack of Effective and Collaborative Public and Private Partnership

Within the Canadian context, a public-private partnership is a cooperative venture among the public and private sectors, built on the expertise of both partners in a fashion that best delivers clearly-defined public needs through the appropriate allocation of resources, risk, and rewards (CCPPP). Implementing suitable security measures and addressing the need for sustainable trade objectives is a challenge for most countries. However, a comprehensive regulatory framework that addresses the majority of the supply chains' activities would reduce the amount of regulatory gaps and overlaps, as well as ensure that trade facilitation is sustainable. Implementing a suitable regulatory framework for marine facilities and ports security could be based on a public-private partnership, which would additionally offer a collaborative and consultative environment. As a

[28] Please refer to section 4.2.2.2. The UK port Security Regulations 2009.
[29] Please refer to section 4.4.6. Canada Small Vessels Security.

result, marine industrial activities would be protected against any interruptions resulting from security threats while also providing a comprehensive regulatory framework. The proposed amendments to the Marine Transportation Security Regulations 2003 are the result of the stakeholders' need to facilitate trade and reduce regulatory burdens. However, decision makers have to collaborate with the public to promote security awareness and enhance the Canadian Maritime security regime by giving stakeholders and the public the time to be adaptable to security requirements. The principle of adaptability would be a good approach to help stakeholders to implement security regulations; accomplishing the aforementioned would establish a balanced security regulatory framework for marine transportation regimes in general.

6.3. Recommendations

The following 4 steps are recommended in order to create the foundation of a sustainable and comprehensive marine transportation security regime for offshore oil and gas installations and mixed-use marine facilities. A short description follows each recommendation.

1. *Create more consistent and proactive regulations; the more you address and prepare for, the less risk there is.*

Establishing a suitable regulatory framework for the protection of marine facilities does not require a new set of security measures. The national and international regulatory frameworks offer several possible approaches for the management of port security; rather, reducing the existing regulatory gaps is key. Doing so would offer a solid foundation to establish suitable regulatory frameworks for marine facilities security. It can be concluded that the Richmond Terminal could improve its protected if TC were to approve the security certificate to categorize it as a fully compliant marine facility. This would ensure that risks associated with ports interacting with unregulated marine industries, such as offshore oil and gas installations, would be greatly reduced.

2. More effective communication with all relevant stakeholders, including but not limited to business representatives.

It should be noted that the marine transportation is a trade-oriented industry. In the business environment, cost reductions are essential for increased profitability. A voluntary enforcement plan for implementing compliance measures could be the best approach. To ensure that measures are voluntarily implemented, communication between authorities, business representatives, and other stakeholders would be needed. Promoting security awareness and giving businesses the time needed for compliance would help industries to adapt to improved security requirements while they maintain business activities. Given that the offshore oil and gas industry is one of the most profitable industries, ensuring the security for offshore supply vessels is priority. Thus, establishing an OUMF without appropriate security plans in place would affect the security of these vessels because they would be subjected to two vulnerable marine sectors. Governments must adopt the public-private partnership approach in order to promote private sector marine security awareness and compliance.

3. Security decisions, development, and regulations should balance the focus of cost minimization and security maximization to prevent losses and consequences

A key element for the success of the supply chain is the security of the chain; creating a strong chain might be costly, though it would ensure sustainability and security.

4. Security and protection of critical infrastructures should be considered at the onset of the planning phase

The Atlantic Gateway and Trade Corridors strategy recognizes the importance of marine security to the supply chain management. Ensuring the sustainability of critical infrastructure requires developers, planners, and decision makers to consider the protection of these assets from

the planning stage in order to avoid any implications or consequences that could result from potential threats[30].

[30] Please refer to The North Atlantic Gateway and Trade Corridor Strategy.2010. Canada's Atlantic Gateway.isbn:978-1-100-50406-3. No.T22-181/2009.Retrieved from Government of Canada form: http://www.atlanticgateway.gc.ca/strategy-index.html

7. Conclusion

To conclude, unregulated marine facilities and non-SOLAS vessels security will remain a gap in the Canadian marine security regime. The flexibility given to vessels that interact with unregulated marine industries imposes additional costs to implement new security requirements as well as creating more operational problems for vessels and mixed-use marine facilities. The most viable and sustainable options include those that reduce the regulatory gaps and overlaps that exist in the current regulatory frameworks. Adopting such options would not only enhance the Canadian marine security regime but would also ensure that trade is more effective and sustainable both domestically and internationally. An effective collaboration between policy decision makers, authority agencies, and stakeholders is needed to facilitate information sharing and addressing regulatory gaps and overlaps. The key objective is to achieve both economic benefits and promote competition by strengthening the national maritime security regime.

8. References

A Good Practice Guide for the Oil and Gas Industry. 2011. Center for the Protection of National Infrastructure (CPNI). Retrieved From CPNI on July 22, 2014 from: http://www.cpni.gov.uk/documents/publications/2011/2011012-gpg_contracting_staff-oil_and_gas.pdf?epslanguage=en-gb

American Association of Port Authorities (AAPA). U.S Public Port Facts. Accessed on July 28, 2014. Retrieved from: http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032

American Association of Port Authorities. U.S and Canadian port Industry Facts. Accessed on July 15, 2014. Retrieved from : http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=993

Association of Canadian Port Authorities .2004.Submission to Transport Canada on Proposed Marine Transport Security Regulations. Retrieved From: www.acpa-ports.net/advocacy/pdfs/formal_submission04.pd

Atlantic Gateway and Trade corridors Strategy (2010). Canada's Atlantic Gateway. ISBN 978-1-100-50406-3. Retrieved from: http://www.atlanticgateway.gc.ca/strategy-index.html.

Australian Customs and Border Protection Service Annual Report. 2008-09. Australian Government. Retrieved from Australian Customs and Border Protection Service on July 22, 2014 from: www.customs.gov.au/webdata/resources/.../annual_report_2008_09.pdf

Australian Government Border Protection Command Fact Sheet. 2009. Retrieved From Customs and Border Protection Service on July 22, 2014 from: www.customs.gov.au/webdata/.../files/MaritimeTerrorismWEB_000.pdf

Avis Peter (2006). Are Canada Offshore Platforms at Risk? Frontline Security. Volume (1), 2. Retrieved from: www. frontline-security.org

Avis Peter. 2006. Is Canada Doing All It Should? Ottawa. Canadian Centre of Intelligence and Security Studies, Carleton University. Volume (3), 2006 of Critical Energy Infrastructure Protection Policy Research Studies. Retrieved from Public Safety Canada on July 3, 2014 from: http://www.publicsafety.gc.ca/cnt/rsrcs/lbrr/ctlg/shwttls-eng.aspx?d=PS&i=76086888

Baines, Simon,. & Syer Tim. 2014. Canada: Important Changes to Canada's Offshore Oil and Gas Regime. Olser, Hoskin& Harcourt LLP. Retrieved from: WWW.OSLER.COM/NEWRESOURCES/IMPORTANT-CHANGES-TO-CANADAS-OFFSHORE-OIL-AND-GAS-REGIME

Bakir, Niyazi.2007. A Brief Analysis of Threats and Vulnerability in the Maritime Domain. Non-published Research Reports. Paper 5. Retrieved from: http://research.create.usc.edu/nonpublished_reports/5

Balancing Security and Efficiency, (2007). The Critical Infrastructure Protection Forum. Dalhousie University. Retrieved From: www.cip.management.dal.ca.

Banomyoun Ruth (2005). The impact of port and trade security initiatives on maritime supply-chain management. Maritime Policy and Management. Vol 32 (1), 3-13. Doi: 10.1080/0308883042000326102

Bateman Sam (2007). Securing Australia's Maritime Approach. Security Challenges. Volume 3 (3). 109-129.

BESS Regions. Bureau of Safety and Environmental Enforcement. Retrieved from: http://www.bsee.gov/About-BSEE/BSEE-Regions/BSEE-Regions/

Brief Overview of the UK National Maritime Security Program. 2008. Department for Transport Guidance. GOV.UK. Retrieved from Gov.UK on July 22, 2014 from: https://www.gov.uk/government/publications/brief-overview-of-the-uk-national-maritime-security-programme

Caldwell Stephen L. 2012. Progress and Challenges 10 Years after the Maritime Transportation Security Act. U.S Government Accountability Office GAO-12-1009T. Retrieved from GAO on July 22, 2014 from: http://www.gao.gov/products/GAO-12-1009T

Caldwell Stephen. 2007. The SAFE Port Act Efforts to Secure Our Nation's Seaports. U.S Government Accountability Office (GAO). GAO-08-86 T. Retrieved from GAO on July18, 2014 from: http://www.gao.gov/products/GAO-08-86T

Canada Marine Transportation security Act (1994). Justice Law Website, S.C. 1994, c.40. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/M-0.8/FullTextAustrali.html

Canada Marine Transportation Security Regulations, (2004). Justice Law Website, SOR/2004-144, Retrieved from: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-144/FullText.html

Code of Practice on Security in Ports (2003). International Maritime Organization/ International Labour Organization. MESSHP/2003/14. Retrieved from: http://www.imo.org/OurWork/Security/Instruments/Pages/CoP.aspx

Container Security Initiative in Summary.2011. U.S. Customs and Border Protection. Retrieved from: http://www.cbp.gov/sites/default/files/documents/csi_brochure_2011_3.pdfDepartment for Transport (2011). Factsheet Maritime Statistics. Retrieved from: http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/70280/maritime-statistics-factsheet.pdf

Development Plan Guidelines (2006). Canada Newfoundland and Labrador Offshore Petroleum Board (C-NLOPB). ISBN 1-897101-15-5. Retrieved from: http://www.cnlopb.nl.ca/pdfs/guidelines/devplan.pdf

Directive 2005/65/European Commission of the European parliament and of the council of 26 October 2005 on enhancing port security. Retrieved on July 15, 2014 from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2005.310.01.0028.01.ENG

Energy Safety and Security Act-Offshore. Natural Resources Canada. Accessed on 15 June, 2014. Retrieved from: http://www.nrcan.gc.ca/media-room/backgrounder/2014/14660

Forbes Andrew (2011). Australian Maritime Economic Interests. Sea Power Centre-Australia. Issue 04, May 2011. Retrieved from: ro.uow.edu.au/cgi/viewcontent.cgi?article=1568&content=lawpaper

Guidance paper on signage and notices. Australian Government .department of infrastructure and transport. Retrieved from: http://www.infrastructure.gov.au/transport/security/maritime/security_plans/files/msz_signage_paper_sep.pdf

Guide to Australian Maritime Security Arrangements (GAMSA). 2013. Australian Border Protection Command, ISBN: 978-0-646-51806-0. Retrieved from Australian Government on July 13, 2014 from: www.customs.gov.au/webdata/resources/files/gamsa_2013_web.pdf

Hansen Ken.2011. The Maritime Security Requirement is Under Appreciated. Canadian Naval Review. Canadian Maritme Security Journal. Retrieved from: http://www.navalreview.ca/2011/07/the-maritime-security-requirement-is-under-appreciated/

Hardy Steven D. 2006. Maritime Security: A Brief Overview. Public Domain. Retrieved from Homeland Security Digital Library on July 28, 2014 from: https://www.hsdl.org/?abstract&did=470425&advanced=advanced

Harel Assaf. 2012. Preventing Terrorist Attacks on Offshore Platforms: Do States Have Sufficient Legal Tools? Harvard Law School National Security Journal. Vol(4). Retrieved from Harvard National Security Journal on 29 July, 2014 from: http://harvardnsj.org/2013/01/preventing-terrorist-attacks-on-offshore-platforms-do-states-have-sufficient-legal-tools/

Haveman J, & Shatz,H (2006). Protecting Nation's Seaports: Balancing Security and Cost. PPIC. ISBN-13: 978-1-58213-120-7. Retrieved from: http://www.ppic.org/content/pubs/R_606JHR.pdf

HIS Global Insight, Inc. (2009). An Evaluation of Maritime Policy in Meeting the Commercial and Security Needs of the United States. Retrieved from: http://www.ihsglobalinsight.com/gcpath/MARADPolicyStudy.pdf

Huang Wen-Chih, et al (2011). The concept of diverse development in port cities. Ocean and Coastal Management. Volume (54). 381-390. Doi: 10.1016/j.oceacoaman.2010.11.004

ILO/IMO Code of Practice on Security in Ports (2010). International Maritime Organization. Retieved on July 16, 2014 from: http://www.imo.org/Ourwork/Security/Instruments/Pages/CoP.aspx

International Ship & Port Facility Security Code and SOLAS Amendments 2002 (2003 Edition). International Maritime Organization. ISBN 92-801-5149-5. Arkle Print ltd. London

Ircha Micheal. 2011. the transportation group UNIVERSITY OF NEW BRUNSWICK. PORTS AND SHIPPING SECURITY. WWW.ctrf.ca/conference/2011gatineau/2011procedengs/11irchaportsecurity.

Kinney Laureen. 2009. Canada's Marine Security. Canadian Naval Review.4 (4). p, 15-19. Retrieved from Canadian Naval Review on 6 June, 2014 from: www.navalreview.ca/wp-content/uploads/.../vol4num4/vol4num4art4.pd.

Marine Security Operations Bulletin-2013-003. Transport Canada. File No :4303-12. Retrieved from: http://www.tc.gc.ca/eng/marinesecurity/operations-bulletins2013-003-416.html

Maritime Security Guidance on Tidal River Thames Passenger Services. Department for Transport. Retrieved from Gov.UK on July 22, 2014 from: https://www.gov.uk/government/publications/maritime-security-guidance-on-tidal-river-thames-passenger-services

Maritime Security Identification Card Scheme. 2014. Australian Government, Department of Infrastructure and Regional Development. Retrieved From the Department of Infrastructure and Regional Development on July 22, 2014 form: https://www.infrastructure.gov.au/transport/security/maritime/msics/index.aspx

Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment, (2006). United Nations, New York and Geneva, 2006. UNCTAD/SDTE/TLB/2005/4. Retrieved from: UNCTAD.org/en/Docs/sdtetlb20054_en.pdf

Maritime Transportation Security Act (MTSA) Course Certification. U.S. Department of Transportation Maritime Administration MARAD. Accessed on 22 July, 2014. Retrieved from: http://www.marad.dot.gov/education_landing_page/mtsa_course_certification/mtsa.htm

Masterangelo Erin. 2005. Overview of U.S. Legislation and Regulations Affecting Offshore Natural Gas and Oil Activity. Energy Information Administration, Office of Oil and Gas, September 2005. Retrieved from: http://www.intellectualtakeout.org/library/primary-sources/overview-us-legislation-and-regulations-affecting-offshore-natural-gas-and-oil-activity

Paola Papa (2013). US and EU strategies for maritime transport security: A comprehensive perceptive. Special issue on transportation pricing policies, Transport Policy. Volume (28). 75-85.Doi: doi: http://dx.doi.org/10.1016/j.tranpol.2012.08.008.

Port Security Requirements.2004. CFN Consultants. Retrieved from: http://www.maritimeawards.ca/pdfs/Port_Security_Requirements.pdf

Preventative Security Guidance for Cruise Ship Visits to Unregulated Places. Australian Government Department of Infrastructure and Regional Development. Accessed on July 24, 2014. Retrieved from: https://www.infrastructure.gov.au/transport/security/maritime/files/preventive_security_guidance_for_cruise_ship_visits_to_unregulated_places.pdf.

Regulatory Impact Analysis Statement.2013. Regulations Amending the Marine Transportation Security Regulations. Canada Gazette. Vol. 147 (17)-April 27, 2013

Rockefeller J. & Thompson, B. 2013.DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy. U.S. Government Accountability Office GAO-14-32. Retrieved from GAO on 22 July, 2014 from: http://www.gao.gov/products/GAO-14-32

Safety Directive, Security of Offshore Installations and Facilities (2011). Canada-Nova Scotia Offshore Petroleum Board. File No 20,100.11. Retrieved from: www.cnsopb.ns.ca/pdfs/Security_Directive.pdf.

Security guidelines for the petroleum industry 2005.American Petroleum Institute API. Retrieved from: http://www.nj.gov/dep/rpp/brp/security/downloads/API%20Security%20Guidance%203rd%20Edition.pdf

Security of Offshore Installations. Transport Canada. Accessed on 15 June, 2014. Retrieved from: https://www.tc.gc.ca/eng/marinesecurity/initiatives-236.htm

Ship Security.2013. Maritime and Coastguard Agency.Gov.UK. Retrieved from Gov.UK on 22 July, 2014 from: https://www.gov.uk/maritime-security

Small Fishing Vessel Security Awareness.2010. Transport Canada. ISBN: 978-1-100-51215-0. No: T29-72/2-2010. Retrieved from: http://publications.gc.ca/site/archivee-archived.html?url=http://publications.gc.ca/collections/collection_2011/tc/T29-72-2-2010-eng.pdf

Stakeholders Report (2013). Halifax Port Authorities. Retrieved from Halifax Port Authority on July 13, 2014 from: portofhalifax.ca/wp-content/.../05/HPA-Stakeholder-Report-2013.pd

The Atlantic Gateway and Trade Corridor Strategy.2010. Canada's Atlantic Gateway.isbn:978-1-100-50406-3. No.T22-181/2009.Retrieved from Government of Canada form: http://www.atlanticgateway.gc.ca/strategy-index.html

The North Atlantic Gateway and Trade Corridor Strategy.2010. Canada's Atlantic Gateway.isbn:978-1-100-50406-3. No.T22-181/2009.Retrieved from Government of Canada form: http://www.atlanticgateway.gc.ca/strategy-index.html

The Parliament of the Commonwealth of Australia. 2005. Maritime Transport Security Amendments Bill. Retrieved From the Pariament of Australia on July 20, 2014 from : http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r2362

The port Security Regulations. 2009 No.2048.Legislaion.gov.uk. Retrieved from The National Archives on 23 July, 2014 from: http://www.legislation.gov.uk/uksi/2009/2048/made

The security Procurement of Contracting Staff. A Good Practice Guide for Oil and Gas Industry (2011). Centre for the Protection of National Infrastructure (CPNI). Retrieved from: http://www.cpni.gov.uk/documents/publications/2011/2011012-gpg_contracting_staff-oil_and_gas.pdf?epslanguage=en-gb

Transport Canada .2011.Canada: Committed to the Goals of International Maritime Community-TP 14916 E (2011). Retrieved from: www.tc.gc.ca/eng/marinesafety/tp-tp14916-menu-182.htm

Transport Canada Recognition Program for Marine Security Training /Courses (Voluntary Program).2007. Transport Canada. Marine Security revision no 01, p 1-6. Retrived from: http://www.tc.gc.ca/media/documents/marinesecurity/tc-recognition-pdfrtf.pdf

Transportation in Canada, Comprehensive Review, (2011). Transport Canada. Minister of public Works and Government Services, Canada, 2012. Cat. No T1-23A/2011-PDF. ISSN 1482-1311. Retrieved From: http://www.tc.gc.ca/media/documents/policy/Transportation_in_Canada_2011.pdf

U.S Maritime Transport Security Act. 2002. Public Law 107-295-NOV.25, 2002. Retrieved from U.S public Law on July 28, 2014 from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf

UK Port Fright Statistics: 2011 Final Figures. Department for transport. Retrieved on Aug 2, 2014 from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/9257/port-freight-statistics-final-2011.pdf

Williams Simon (2013). Offshore Installations: Practical Security and Legal Considerations. Centre for International Maritime Security. Retrieved From: cimsec.org