The Maritime Security Regulations: do they go far enough?

F. A. Anstey[1]

Abstract

The Diplomatic Conference on Maritime Security held in London in December 2002 adopted the International Ship and Port Facility Security Code for the purpose of detecting and deterring security threats to the maritime transportation sector. However by failing to institute a broader application, the maritime community has been lulled into a false sense of security. The International Maritime Organization insists that risk assessment is an essential and integral process for ships and facilities when developing requisite security plans but it has not used the same criteria when identifying applicable ships for inclusion within the Code. Although terrorist attacks are frequently directed at oil related infrastructure and personnel, the apparent lobbying efforts of the oil industry have resulted in the exemption of assets, such as the Floating Production Storage and Offloading vessel, and most Mobile Offshore Drilling Units, from the mandatory application of the ISPS Code. The potential consequences of an attack on these high value assets are significant loss of life, appalling environmental damage, and economic disruption through supply shortages and volatile oil price fluctuations. Fishing vessels too have been excluded. Thousands of deep-sea trawlers of significant tonnage, ply international waters, have multinational crews, and visit ports worldwide, but are not included in the security regulations and therefore remain off the radar screen of international security inspectors. At best they pose a risk of contaminating ISPS certified ships and port facilities, at worst they can be used to cause a major security incident. Similarly large ocean-going yachts have been exempted from the ISPS Code, creating security risks and indeed have been used for eco-terrorism activities. High-risk government vessels, attractive to terrorist organizations are also exempt from the security regulations. A variety of application measures are being used by some contracting governments, with national security regulations applying to an array of smaller type vessels, and with some including domestic-trade vessels. Most countries have ignored home-trade passenger ferries, which may carry hundreds of passengers

[1] Faculty – Maritime Security, School of Maritime Studies, Fisheries and Marine Institute of Memorial University, PO Box 4920 St. John's Newfoundland A1C 5R3 Canada, +1.709.778.0581, Fred.Anstey@mi.mun.ca

and vehicles, and create an obvious target for terrorist organizations. Additional risk is incurred because contracting governments have not used standardized criteria for conducting background security checks for port facility and vessel personnel. This paper has conducted a literature review, and an analysis of pertinent statistics and security regulations to examine the risks associated with these insufficient measures.

1. Introduction

The ISPS Code identifies the mandatory security requirements to be enforced by contracting governments and other affected parties. The application section of the Code is central to this security regime as it identifies the ships and consequently the port facilities to which the Code applies. It requires passenger vessels, certain cargo ships and mobile offshore drilling units (MODUs) that are on international voyages, to conform. The IMO has used the guidance in Part B, the amendments to the SOLAS Convention and the issuance of circulars to clarify many of the requirements of this international security framework. A stated ISPS Code objective (IMO 2003a) is, "to ensure confidence that adequate and proportionate maritime security measures are in place." The arbitrary selection of vessels and associated port facilities does not totally meet this objective. A review of the included and excluded categories of vessels reveals a number of short-comings, not easily fixed through national security regulations. This fact, combined with the inadequate, unregulated personnel identification system for seafarers and port facility workers, has resulted in a piecemeal global security regime with weaknesses that may ultimately defeat the intent of the Code.

2. Vessel size

Vessel tonnage is one criterion used to determine cargo vessels that are required to comply. It is an arbitrary determinant, of 500 gross tonnage and upwards, and is not directly linked to maritime security considerations. In reality, and as indicated by the Code, the implementation of a security regime must be based on a security risk assessment. The security regulations, by applying this arbitrary cut off has exempted smaller sized vessels, which due to the nature of their work or the nature of their passage may indeed pose a risk that exceeds that of larger vessels. Secretary-General Mitropoulos (2005) of the IMO, in an address to a seminar on maritime security stated that "the threat of a small craft might even be greater than that posed by SOLAS ships" and he further admitted that such an incident "could have a major disruptive effect on human life, the environment and local, regional and even international trade".

Several countries have moved to address the potential threat of non-SOLAS ships. The port of Singapore, having 3000 small vessels that operate in and around its harbour, has implemented a number of security measures. They include the requirements to carry a low-cost transponder, to complete a ship security self-assessment, and to abide by a Harbour Craft Security Code (Yew 2005). Other countries, in national security legislation, have used a smaller gross tonnage as the arbitrary cut off for applicable ships. The United States has included foreign cargo vessels and self-propelled U.S. cargo vessels, greater than 100 grt, in its Maritime Transportation Security Regulations (MTSR). Transport Canada (2007) has defined 'non-SOLAS ships' as those engaged on a voyage from a port in one country to a port in another country and in excess of 100 grt, and identified them for inclusion in the Canadian MTSR.

These examples are not suggested to be the ideal models for determining the appropriate size of vessels for inclusion, but they do indicate that the arbitrary tonnage requirement, as mandated by the ISPS Code does not address all security concerns. The IMO (2004b) identified 22,500 vessels requiring ISPS compliance, but according to the Institute of Shipping Economics and Logistics (ISL 2002) the total merchant fleet comprised of about 90,000 vessels of 100 grt and over. The Code, through Part B, does suggest that vessels less than Convention size may be subject to controls imposed by port states, but as this section is designated non-mandatory, adherence is envisioned to be sporadic at best.

The IMO (2003a), through SOLAS, now requires that certain vessels be fitted with an Automatic Identification System (AIS). From a security perspective this will enable other vessels and port states equipped with AIS receivers to determine, in part, the identity of those vessels. The regulations also require that certain ships be outfitted with a ship security alert system (SSAS) to enable them to alert a competent authority, when they are the subject of a security incident, in order that a response may be initiated. Respectively, these regulations apply to vessels of 300 grt and 500 grt and upwards and therefore vessels of a smaller size are not required to be outfitted. When analysing the infamous attacks on the USS Cole and the VLCC Limburg, or the hundreds of piracy attacks that occur annually, it becomes apparent that small vessels are often the threat and without including AIS requirements for these vessels, all such ships may be viewed with suspicion. Additionally, it is not always large vessels that are subjected to security incidents, particularly in areas where piracy is prevalent, and smaller vessels may also benefit from the mandatory carriage of SSAS.

3. International Voyages

The ISPS security measures apply to certain vessels on an international voyage, defined by SOLAS as a voyage from one contracting country to a port outside that country. This suggests that the risk of a security incident can only be caused to, or through vessels coming from that other country. The 'international voyage' definition (IMO 2004c) also precludes vessels navigating solely on the Great Lakes and St. Lawrence River, even though such voyages commonly involve passage between the United States and Canada. These two countries, recognizing the risks associated with this exclusion have included these voyages within their national security regulations. The United States (USCG 2003) has also expanded the list of applicable ships to accommodate those domestic vessels considered to be of higher risk, such as those carrying more than 150 passengers, and vessels or barges carrying certain dangerous cargoes.

It is difficult to determine the extent of the risk caused by the exclusion of domestic trade vessels. However on the ISPS Code implementation date, IMO (2004b) calculated that 22,500 vessels were required to be compliant. According to world fleet statistics as cited by the Japan International Transport Institute (JITI 2005) the global merchant fleet of vessels of 500 grt and over totalled in excess 45,500 vessels. Therefore it may be inferred that there were just as many vessels of this size that were engaged on domestic voyages, and to which the Code did not apply. The IMO also noted that 9000 port facilities, servicing ISPS certified vessels, were required to conform to the Code. The significant number of domestic vessels suggests that there are also a large number of facilities not requiring compliance even if the ship or facility is a high risk asset, because it does not service vessels that are on international voyages.

Some jurisdictions have realized the risks associated with using only the international voyage as a determinant for their security regulations. The European Parliament (2004), while following the ISPS model for initial implementation, phased in other applicable vessels in years following. By 2005 the regulations applied to Class A domestic passenger ships and in 2007 they affected certain other vessels operating domestically. The EU regulations mandated that countries within the European Union conduct a security risk assessment to determine precisely which vessels would be covered, and this process is envisioned to suffice if all countries apply a rigorous and consistent risk assessment model. Additionally, as the regulations have expanded the categories of vessels requiring certification they also require port facilities servicing those vessels to comply with the security regulations.

It is interesting to note that terrorist attacks have commonly been carried out against domestic transportation systems. High profile examples, including the use of American aircrafts in the attacks of 9/11; the targets of domestic commuter trains in Madrid in 2004; and the attacks on the London bus and subway systems in 2005, all point towards the risk to domestic transportation. These events suggest that the maritime community

has also incurred an elevated risk because it has not mandated consistent global security procedures for domestic trade vessels and associated port facilities.

4. Passenger Ships

Passenger vessels are at risk as evidenced by the notorious terrorist attack on the Achille Lauro and the high-profile pirate attack on the Seabourn Spirit (BBC 2005). The cruise ship industry is of particular interest and statistics (ISL 2002) indicate that the number and size of vessels within this industry continues to grow. A major security incident has the potential to cause significant loss of life, the destruction of the vessel and port facility, and the economic crippling of an industry. As the size of theses vessels increases, and with their capability to carry more crew and passengers, the attractiveness as a target also increases.

However, in addition to the cruise ship industry there are other vessels that carry passengers including cargo and Ro-Ro passenger ships, and ferry vessels. The Code has recognized the inherent risk and for that reason has not used vessel size as a determinant. Rather for security purposes it encompasses vessels carrying more than 12 passengers while on an international voyage. However domestic ferries are not covered by the Code and do not have the resultant security plans and procedures. Unfortunately, as evidenced by attacks in Manila on the Superferry 14 in 2004 killing 116 people, and on the Dona Romona in 2005 killing two, such vessels are not immune from the aggression of terrorist organizations (Martin 2005).

In Canada, BC Ferries (2007) has a fleet of 36 vessels servicing 47 ports of call. The largest is 560 feet in length, capable of carrying 2100 passengers and 470 vehicles. In 2005/06 the fleet carried in excess of 8.5 million vehicles and 21.7 million passengers on over 186,000 sailings. As the voyages conducted by these vessels are not international, the vessels are not required to comply with the international security regulations, even though a major security incident on one of these vessels would not be viewed as any less significant. Globally, statistics indicate that there are about 3800 vessels, excluding cruise ships, categorized as passenger vessels (ISL 2002). A major security incident on this type vessel whether domestic or international would have major implications.

5. Fishing Vessels

As wth SOLAS the security Code does not embrace fishing vessels. Statistics gathered by the Institute of Shipping Economics and Statistics (ISL 2002) establishes the global fishing fleet of vessels over 100 grt, at over 23,000. Globally, it is estimated that there are 15 million people working aboard fishing vessels. While these statistics do not give a breakdown of size, category or type of trade, there are a sizable number of such vessels and individuals engaged in the deep-sea and international trade. For example in 2005 the Pacific Island Region, which requires foreign fishing vessel registration, 1100 such vessels were registered (Martin 2005).

Fishing vessels frequently conduct foreign port visits for cargo discharge, replenishment, repairs, and relaxation. The fact that these vessels are not covered by the ISPS Code is cause for concern. In New Zealand, the Director of Maritime Safety (Kilvington 2004) noted that some fishing vessels carry far larger crews than cargo vessels, and he stated that New Zealand border control agencies have increasing become aware of irregularities pertaining to fishing vessels. Consequentially this jurisdiction may advocate an amendment to the ISPS Code to incorporate 'international' fishing vessels for application.

A common concern even with ISPS compliant vessels surrounds adequate and reliable crew identification. The Seafarer Identification Document (SID) is one solution considered by port states to alleviate this concern. The intent of the SID is to facilitate the movement of seafarers when joining and leaving ship or going ashore. The use of recognized identification and the additional controls placed upon ISPS vessels by the port state and by port facilities has ensured some degree of control over the movement of seafarers. However such controls are not as prevalent within the fishing industry. Too frequently such vessels will berth at facilities which are not ISPS compliant, and that are not required to monitor the movement of persons to and from the vessel. The extent and quality of checks carried out regarding crew identification and even crew numbers is widely acknowledged to be very poor and therefore has caused some observers to describe this industry as the potential Trojan Horse of maritime security (Martin 2005).

Fishing vessels are also exempt from the AIS carriage requirements. Additionally the Long Range Information and Tracking (LRIT) regulations, which come into effect January 1st, 2008, will not apply to fishing vessels. This regulation requires applicable vessels to be outfitted with a LRIT system that enables SOLAS governments to receive information about ships navigating within a distance of hundreds and even thousands of nautical miles off their coast. As fishing vessels are exempt from the carriage of LRIT and AIS it will make it difficult to monitor their movements as compared to vessels that are so equipped.

The new security measures (IMO 2003a) necessitated amendments to the SOLAS Convention including the requirement for ships to prominently display their unique IMO number. The regulations specify color, size and location of these permanent mark-

ings. Additionally SOLAS vessels are now required to carry a Continuous Synopsis Record (CSR). This document is intended to provide an onboard record of the vessel's history as of July 1st, 2004. It is kept onboard and is subject to inspection by port state control officers. The intent of both the IMO number display and the CSR are to combat the use of 'ghost ships' that have been used to stymie various international regulations. Port state control officers will now have additional tools to ensure that vessels no longer misrepresent themselves. Unfortunately, as fishing vessels are excluded from the SOLAS Convention they are not required to display such identification or carry the CSR and their ability to more easily circumvent various regulations will continue.

The exemption of fishing vessels also provides complications for many ports and port facilities. During a visit by such vessels, facilities will have to ensure that there is no violation of the port facility security plan or 'contamination' of other interfacing vessels. The fishing vessel has no ship security plan to violate, but the actions of the crew could cause a security breach, threat, or incident that could have severe repercussions for that facility.

Research by Martin (2005 cited ICONS 2005) pertaining to the fishing industry, determined that many crew members work under conditions of extreme hardship. It also found that, globally, they were not well organized and often not covered by international labour and safety standards. Quite frequently crews were found to be poorly paid and from poor, undeveloped parts of the world. Conditions onboard fishing vessels were found to be 'fertile grounds for resentment and dissent' and in the broader context of maritime security and when viewed in conjunction with other problems as previously identified, the exclusion of fishing vessels from the security regulations should be viewed with concern.

6. Yachts

A number of similar concerns are raised due to the fact that pleasure craft are also exempt from the security regulations. The fact that there are an incalculable number of such vessels, often having the ability to berth at small and even undisclosed locations, and with some frequently on international voyages, is disconcerting. These vessels are not required to be equipped with AIS or LRIT and do not display IMO numbers or make use of the CSR. By definition such vessels are normally used for pleasure and as such frequently travel without the use of passage plan, with sudden changes of destination, and without following many regulations that merchant vessels are required to follow.

Some eco-terrorism groups have been accused of thwarting international regulations by declaring vessels used in their operations as 'yachts' and therefore exempt from many regulations. The R/V Farley Mowat originally built as a Norwegian fisheries research and enforcement vessel was registered under the Canadian flag as a pleasure

craft and therefore not required to carry safety, security or manning certificates. The vessel, of significant size at 677 grt and engaged in international travel, was accused of harassing several Japanese fishing vessels engaged in the whale fishery (Baron 2007). This scenario could easily be played out by other terrorist organizations with more sinister results.

7. Government vessels

Warships, naval auxiliaries, and ships owned or operated by governments for non-commercial use are specifically exempt from the requirements of the ISPS Code. The high profile attack on the USS Cole in Yemen in 2000 underscores the risks to such vessels. For many such vessels, particularly warships it is expected that they will institute measures that meet or exceed the Code. However the category of ships 'operated by governments for non-commercial use' could include many vessels that would not have comparable security measures.

Another problem is that exempted vessels may not have appropriate security procedures in place when interfacing with port facilities or other vessels. ISPS compliant facilities will have procedures for the acceptance of ship stores bunkers and cargo, and for access control measures. Compliant vessels will have similar procedures which dovetail with the port facility procedures. Anecdotal evidence, gathered during marine security training courses, suggests that exempted vessels are often unaware of such procedures, due to the lack of knowledge of the security regulations and therefore do not readily conform to facility procedures creating at best complications for such facilities and at worst causing security breeches which must be reported to the appropriate authorities.

The blanket exemption of such vessels from the security regulations appears to be a matter of convenience for contracting governments that causes complications for others that are required to adhere to those regulations.

8. Oil industry maritime assets

The ISPS Code, in Part A, does give some degree of comfort that high value oil industry assets will be protected, as it includes the mobile offshore drilling unit (MODU) in the definition of ship and specifically states that the Code is to apply. However SOLAS Chapter XI-2 states that by definition the MODU is to be so designated for the purpose of maritime security only if it is mechanically self-propelled and not on location. Most MODUs are not self-propelled and instead require the use of support vessels to tow them from location to location. The purpose and design of a MODU is for oil exploration

and this entails that it spend most of its time on location. Additionally while engaged in exploration the MODU would see a full complement of workers and use a range of dangerous goods necessary for its work. It is therefore envisioned that at any given time the global MODU fleet, numbering 920 in 2006, would not be required to implement the ISPS Code even though these assets represent high value, have a large complement of employees and do present an attractive target (IUMI 2006).

The oil industry also uses floating production, storage, and offloading units (FPSOs), and floating storage units (FSUs) in the process of bringing hydrocarbons from field to market. Again these assets are of high value, have a large crew complement, and indeed resemble large vessels. Through MSC/Circ. 1097/1111, the IMO (2003b/2004a) has decided that neither of these is to be classed as ships for the purpose of ISPS Code application. The only concern expressed through the circulars is that ISPS compliant vessels interfacing with a FPSO/FSU would be considered 'contaminated' because the installation was not required to be compliant. There is no direct security concern iterated for the FPSO/FSU.

To put this matter in perspective it is interesting to look to the east coast of Canada for an example of the possible ramifications of following only the mandatory requirements of the ISPS Code. Canada accounts for about 10% of the United States crude oil needs and is second only to Saudi Arabia in estimated oil reserves. In 2006, the offshore oilfields of eastern Canada produced over 110 million barrels of oil, representing 13% of the total Canadian crude production (Rowat 2006). This product was recovered using the Hibernia Platform, the SeaRose FPSO, and the Terra Nova FPSO. In total the construction cost of these assets is about eight billion dollars, their total combined crew complement is over 400 persons, and total crude oil storage capacity is 2.2 million barrels of crude oil. A number of MODUs continue to be used to delineate the oil fields. Several shuttle tankers transport the crude to a transhipment terminal in Canada, while others transport direct to market in the United States. Canadian flag offshore supply vessels service all three installations. In this scenario, the ISPS Code would only be mandatory to the tankers that travel to the United States. All other assets would be outside the purview of these regulations and therefore security procedures would not be required. An attack on such assets could result in significant loss of life, have catastrophic environmental impact, and cause a serious disruption in oil supply and create havoc in world oil and financial markets.

The scenario as previously iterated is of a significant security concern and as expected the Canadian government has instituted national security provisions for these oil fields. Likewise the United States has mandated security requirements for the outer continental shelf to cover assets such as MODUs and fixed and floating assets not covered by the Code. However the fact that the ISPS Code, the primary maritime security document, does not apply to these assets, and the fact that such high value assets require that applicable jurisdictions mandate security requirements, undermines the

Code objective of "detecting security threats and taking preventative measures against security measures" that affect the maritime industry (IMO 2003a). Other jurisdictions may not be as vigilant when instituting domestic security measures.

Security procedures, plans and measures are to be based on risk assessment, and the ISPS Code espouses as one of its objectives the importance of ensuring confidence that adequate and proportionate maritime security measures are in place. However the fact that these high value assets, belonging to an industry that have evidenced terrorist attacks, such as the foiled attack on a major oil production facility in Saudi Arabia (Gardner 2006) and the attack on the VLCC Limburg, are not covered by the Code does not portray a seamless, effective security regime.

The oil industry in general is a target of interest for terrorist groups. Osama bin Laden, the world's most notorious terrorist has stated that the oil industry is the 'umbilical cord' of the western world. The fact that certain assets are not covered by the Code provides a gap in the security measures and one security analyst has stated that "Al Qaeda is very, very good at identifying gaps" (Murphy 2003).

9. Identification Documentation

The ISPS Code was developed primarily for the protection of ships and port facilities. A cornerstone of both the ship and the port facility security plan is the procedure for access control. The complexity of the shipping industry necessitates frequent movement of persons to and from the ship and facility and therefore each of these entities is required to establish procedures for appropriate identification as part of these mandated access control measures.

Without the comfort of a recognized system of identification documentation, port states have been concerned with the movement of seafarers during port visits. There has been considerable discussion surrounding the requirements for appropriate seafarer's identification documentation (SID) in order to ensure that individuals have been appropriately vetted and that the resultant documentation is issued. The International Labour Organization (2003) has, through its Seafarers' Identity Documents Convention, created a system for the issuance of a recognized SID. This convention outlines procedures for the issuance of the document, for the protection of national databases, and it also outlines the content and form requirements.

The revised convention, in effect as of February 2005, leaves much work to be done to ensure worldwide acceptance. Although there are still problems associated with seafarer identification, there does at least appear to be a willingness to address these issues. One of the concerns with the convention is that it does not direct governments to do a risk assessment on individuals who apply for such documentation, but rather it focuses only on confirmation that the person has reliable and verifiable documenta-

tion. Some countries, such as Canada and the United States, recognizing this concern now require significant background checks for those applying for this documentation to determine if the individual poses a security risk to the maritime industry.

In contrast, there has been no concerted effort to promote a global system for identification documentation for port facility workers. A survey conducted by the International Chamber of Shipping and reported by IMO (2006), raised significant concerns related to port facilities. Some facilities had PFSOs that were conspicuous by their absence, others remained unresponsive to calls for help by vessels at the facility, and there were instances of even officials refusing to show identification, or to wear a visitor's pass. The idea of port workers having applicable security clearance and resultant identification at such ports appears not to be even on the radar. The survey concluded that these shortfalls jeopardized the broad effort of maritime security and that it increased the burden of ships and crews.

Some countries however have determined that port facility workers, by having access to sensitive areas, may pose a risk to ships and other marine assets. The United States uses the Transportation Worker Identification Credential (TWIC) as identification for all such personnel requiring access to secure areas. Individuals that require unescorted access must pass a security threat assessment as conducted by the Transportation Security Administration (TSA 2006), before receiving clearance and subsequent identification. Similarly, Canada has the Marine Transportation Security Clearance Program (MTSCP), which does similar risk assessment but on a limited number of workers (TC 2006). Many other countries have no such program.

The global tendency to emphasize the need for seafarer identification while ignoring the need for similar identification for port and port facility workers appears to defeat the purpose of the security regulations. It suggests that although the ISPS Code places equal importance on enforcing preventative measures against security incidents affecting ships and port facilities, in reality it is the ship that is left vulnerable. The varying national standards, as illustrated, for both ship and port facility identification do not produce a reliable identification system that is consistently based on risk assessment and therefore provides further gaps in the global security arrangement.

10. Summary

This paper has identified a number of areas of concern with regards to maritime security. There is a need to expand the application of the ISPS Code to other vessels and to the domestic trade. Exactly how these vessels should be included is difficult to say. However, as illustrated the categories of vessels reviewed each pose security challenges. Smaller vessels often stay in one geographic area and one study (JITI 2005) has suggested the registration of non-SOLAS vessels on a regional basis. Areas with higher

risk of security incidents, including important international straits, will require more stringent measures.

Large passenger vessels whether on domestic or international travel are attractive targets for terrorist organizations and should be included in the Code. The FPSOs and other oil industry assets are conspicuous by their absence from mandatory inclusion in the Code. Whether MODUs are on location or self-propelled is immaterial. Risk assessment demands that such assets also be included.

Government classed vessels should require security measures possibly under a different authority but mirroring the requirements of the Code. More concern must be shown for the yachts and fishing vessels that move about almost as if unseen. The risks, as identified, need to be addressed. Both types of vessel should be considered for carriage of the AIS or similar transponder device. The inclusion within the Code of the categories of vessels discussed will also entail the certification of more port facilities.

A recognized system of identification documentation for both seafarers and port facility personnel is requisite. The vessels discussed are in themselves not the danger. The danger lies with the people that move through our ports and on our vessels. This issue is paramount for maritime security.

The development and implementation of the ISPS Code was primarily a result of the events of 9/11. It was a quick response by the IMO to perceived maritime security threats. This implementation, although not without short-comings, has required the global community to grapple with the issue of maritime security. The ISPS Code insists that security officers maintain the continued effectiveness of the security plan through audits, amendments and response to any identified deficiencies. This is advice that the IMO itself should follow for improving the International Ship and Port Facility Security Code.

References

1. Baron, E., 2007. Eco-activist claims harassment in ship status fracas. Canwest News Service. [online]. Available from:
2. http://www.canada.com/topics/news/national/story.html?id=89efaf16-b353-4297-ba60-dd2a7c326f84&k=23675 [Accessed 28 June 2007].
3. BBC News, 2005. Cruise ship repels Somali pirates. BBC News. [online].
4. Available from: http://news.bbc.co.uk/2/hi/africa/4409662.stm
5. [Accessed 28 June 2007].
6. BC Ferries, 2007. About BC Ferries [online]. Available from: http://www.bcferries.com/
7. [Accessed 27 June 2007].
8. European Parliament, 2004. Regulation (EC) No 725/2004 of the European Parliament: on enhancing ship and port facility security. Official journal of the European Union. [online]. Available from: http://www.mcga.gov.uk/c4mca/ec_no_725_2004.pdf

9. [Accessed 26 June 2007].
10. Gardner, F., 2006. Saudis 'foil oil facility attack' BBC News. [online]. Available from: http://news.bbc.co.uk [Accessed 27 June 2007].
11. Institute of Shipping Economics and Logistics (ISL), 2002. Shipping statistics yearbook 2002.
12. Bremen: ISL.
13. International Labour Organization (ILO), 2003. Seafarers' Identity Documents Convention (Revised). http://www.ilo.org/ilolex/cgi-lex/convde.pl?C185
14. International Maritime Organization, 2003a. ISPS Code. London: Halstan.
15. International Maritime Organization, 2003b. MSC/Circ. 1097: Guidance relating to the implementation of SOLAS chapterXI-2 and the ISPS Code. London: IMO.
16. International Maritime Organization, 2004a. MSC/Circ. 1111: Guidance relating to the implementation of SOLAS chapterXI-2 and the ISPS Code. London: IMO.
17. International Maritime Organization, 2004b. ISPS Code status update 05. [online]. London, IMO. Available from: http:www.imo.org/Newsroom [Accessed 26 June 2007].
18. International Maritime Organization, 2004c. SOLAS consolidated edition 2004. London: IMO.
19. International Maritime Organization, 2006. MSC 81/5/15: Measures to enhance maritime security. London: IMO.
20. International Union of Marine Insurance (IUMI), 2006. Report on world merchant fleet. [online]. Zurich, IUMI. Available from: http://iumi.svv.ch/ [accessed 26 June 2007].
21. Japan International Transport Institute (JITI), 2005. A study on maritime security measures for non-SOLAS vessels. Tokyo: JITI.
22. Kilvington, R., 2004. The ISPS Code and beyond. [online]. The Maritime Law Association, Australia. Available from:
23. http://esvc000873.wic005u.server-web.com/docs/11%20Russell%20Kilvington.pdf
24. [Accessed 27 June 2007].
25. Martin, T., 2005. Report on foreign fishing vessel security in the pacific island region. Suva: Secretariat of the Pacific Community.
26. Mitropoulos, E., 2005. Opening address to the seminar on maritime security measures for non-SOLAS vessels [online]. London, IMO. Available from: http://www.imo.org/Newsroom/
27. [Accessed 26 June 2007].
28. Murphy, K. 2003. Oil industry is an obvious terrorist target say experts. Daily Times. [online]. Available from: http://www.dailytimes.com.pk/default.asp?page=story_19-4-2003_pg4_22
29. [Accessed 27 June 2007]
30. Rowat, M.R., 2006. Boom times: Canada's crude petroleum industry. Ottawa: Ministry of Industry.

31. Transport Canada (TC), 2006. Marine transportation security regulations. [online] Ottawa, Government of Canada. Available from: http://www.tc.gc.ca/acts-regulations
32. [Accessed 25 June 2007]
33. Transportation Security Administration (TSA), 2006. TWIC Final Rule Guidance. Washington: DHS.
34. United States Coast Guard (USCG), 2003. Code of federal regulations. Washington: DHS.
35. Yew, L.T., 2005. Maritime security measures for non-SOLAS vessels. Seminar on maritime security measures for non-SOLAS vessels, 10 May 2005 London.