

New Measures for Maritime Security Aboard Ships and in Port Facilities

by

**Captain Dr Peter Heathcote¹
Regional Maritime Legal Advisor
Secretariat of the Pacific Community
Suva, Fiji Islands**

The Background

Following the terrorist atrocities of 11 September 2001, the Assembly of the International Maritime Organization (IMO) in November 2001 unanimously agreed to the development of new measures relating to the security of ships and of port facilities, for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 1974) in December 2002. This Conference adopted new provisions to SOLAS 1974 and the International Code for the Security of Ships and of Port Facilities (ISPS Code). These new requirements form the international framework through which ships and port facilities can cooperate to detect and deter acts that threaten security in the maritime transport sector.

Terrorism and Piracy

Terrorism was not a new phenomenon, and the IMO has been looking into the issue of security at sea since the takeover by Palestinian terrorists of the Italian passenger ship *Achille Lauro* in 1983, when an American passenger was killed and his body thrown overboard.² In subsequent years, piracy and the highjacking of ships and their cargoes became more frequent and more pervasive, endangering the lives of seafarers and putting at risk theft of cargoes worth millions of dollars.

IMO Response

In 1985, the IMO adopted Assembly resolution A.545(13), “Measures to prevent acts of piracy and armed robbery against ships”, to address the specific problems relating to these issues. Then, in September 1986, the Maritime Safety Committee (MSC) approved MSC/Circ.443, “Measures to prevent unlawful acts against passengers and crew on board ships”, intended for application to passenger ships engaged on international voyages of 24 hours or more and the port facilities which service them. This was an interim measure until the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 (SUA) came into force. Then, in 1996, came MSC/Circ.754, entitled “Passenger Ferry Security”, relating primarily to passenger ferries operating on international routes and the ports serving those routes. The circular stated that the measures might “also be applied to international freight ferry operations depending on the requirements of individual Member Governments.” There are inconsistencies between the two circulars.

The SUA Convention

Eventually the IMO was requested to draw up a convention on the subject of unlawful acts against the safety of maritime navigation. The proposed convention was to provide for a comprehensive suppression of unlawful acts committed against the safety of maritime navigation that endanger innocent human lives, jeopardise the safety of persons and property, or seriously affect the operation of maritime services, which are of grave concern to the international community as a whole. This resulted

in the adoption, in March 1988, of the SUA Convention. A later Protocol of the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 1988, extended the provisions of the convention to unlawful acts against fixed platforms located on the Continental Shelf. These two instruments entered into force on 1 March 1992 and both are quite widely ratified, including three Pacific Island countries – Marshall Islands, Palau and Vanuatu - the first and last of which operate “Open Registries”.

The main purpose of the SUA conventions is to ensure that appropriate action is taken against persons committing unlawful acts against ships (and fixed platforms on the continental Shelf), which include the seizure of ships by force, acts of violence against persons on board ships, and the placing of devices on board a ship which are likely to destroy or damage it. The treaties oblige Contracting Governments either to extradite or prosecute alleged offenders.

So why SOLAS?

So why, if there is a convention dealing with measures to protect ships, ship’s crews, passengers and cargoes from unlawful acts at sea (SUA), clearly matters of security, was an amendment patently to do with enhancing security introduced through a convention that obviously deals with safety (SOLAS)?

The answer is - in order that the provisions could be implemented quickly. Most conventions contain certain general principles in Articles, as well as issues standard to almost every convention (provisions for signature, ratification and acceptance, as well as provisions concerning revision of the Convention and the introduction of amendments). These Articles do not often require amending. The main technical provisions of the convention are usually contained in Regulations, Annexes or Appendices. It is these that often require frequent amendment. In view of the long time it took in the past to bring amendments into force, it was realised that what was required was a formula whereby amendments to the technical provisions could be made by a more streamlined process. The new formula was known as the “Tacit Amendment Procedure” where amendments would enter into force on a specific date contained in the amendment, unless a certain specified number of States objected to the provisions. In other words, silence would be deemed to be acceptance. No further action would be required if a State approved of the new measures. The SOLAS Convention contains a “tacit acceptance procedure” whereas the SUA Convention does not. Therefore the proponents of these new security measures felt that SOLAS had to be the vehicle to implement them as soon as possible. Furthermore, the existing SUA Convention deals with issues that were raised by the *Achille Lauro* hijacking and deals with international cooperation in bringing terrorists to justice, such as expediting extradition, whereas the new SOLAS provisions incorporate the International Ship and Port Security (ISPS) Code and are primarily in response to the events that took place on 11 September 2001. The ISPS Code deals with a whole range of measures, including access control, vetting and identification requirements, and even deals with port facilities.

What is Terrorism?

There are no internationally agreed definitions for the terms “terrorism” and “terrorist”. However, the United Kingdom Prevention of Terrorism Act, 1976 defines terrorism as the “use of violence for political ends [including] violence for the

purpose of putting the public or any section of the public in fear.” Furthermore, the United States Department of State has defined terrorism as “premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine state agents.” Maritime security consists of those measures employed by owners, operators and administrators of vessels and ports to protect against terrorism, sabotage, stowaways, illegal immigrants, asylum seekers, piracy and armed robbery at sea, seizure, pilferage, annoyance and surprise.

Awareness Raising

A workshop, sponsored by the IMO and organised by the Australian Maritime Safety Authority (AMSA) with assistance from the Secretariat of the Pacific Community (SPC), was held in Sydney, Australia, from 2 to 6 September 2002. The purpose of the Workshop was to raise awareness of maritime and ports personnel in government and industry to local acts of terrorism in ports, on ships in ports and on ships at sea, and recent initiatives taken by the IMO to combat the menace. Delegates from 14 Pacific Island countries attended the workshop. The meeting recognised the importance of the multi-modal transportation chain and observed that increased security might increase costs, but that increased security could benefit shipping and ports by reducing the incidence of pilferage, piracy, armed robbery at sea, people smuggling and stowaways. Pacific Island delegations were concerned that the “tacit acceptance” procedures would force the proposed changes on them within a short time-frame, which could be costly to implement. Also of concern was the question of the application of the new “mandatory” security measures, since SOLAS dealt with ships on international voyages whilst the new measures seemed to deal with passenger ships and cargo ships of 500 gross tonnage and over, irrespective of whether they were engaged on an international voyage or not. The convenors of the meeting hoped governments would enact the provisions of the new Code being developed, and the IMO offered advice and assistance.

Other Responses

At this stage, prior to the Diplomatic Conference held at IMO headquarters in London from 9 to 13 December 2002, delegates to the workshop were advised that some of the issues were still open for debate, including seafarers’ background checks, determination of container contents, and transparency of ownership of ships. Final agreement was also being sought on issues including: Automatic Identification Systems (AIS) on all ships, the IMO number to be painted on the side of all ships, and internal and external alarms to be fitted and activated in the event of an attack on the ship. Discussion at the workshop concentrated more on port security than on ship security, but looked at the direct operational interface with the ship, with the recommendation that the port facility interface should be kept as small as possible. There was much discussion of what that might mean in Australia, but one delegate pointed out that ports in the Pacific, such as Suva, Apia and Nuku’alofa were quite different and had different problems from ports such as Brisbane and Sydney. This was recognised, and it was agreed that the solution would be “what was reasonable in the circumstances”.

The Conference

Thus, at the Diplomatic Conference held in December 2002, amendments were made to the existing provisions of SOLAS, accelerating the implementation of the requirement to fit Automatic Identification Systems and adopt new Regulations in

Chapter XI-1 of SOLAS 1974 covering marking of the Ship's Identification Number and the carriage of a Continuous Synopsis Record. The provisions of Chapter XI-2 of SOLAS 1974 and the ISPS Code apply to ships and to port facilities. The extension of SOLAS to cover port facilities was agreed on the basis that SOLAS 1974 offered the speediest means of ensuring the necessary security measures entered into force and were given effect quickly. However, it was further agreed that the provisions relating to port facilities should relate solely to the ship/port interface.

Implementation of the provisions will require continuing effective co-operation and understanding between all those involved with, or using, ships and port facilities including ship's personnel, port personnel, passengers, cargo interests, ship and port management and those in domestic agencies and organizations with responsibility for national and local security. Existing practices and procedures will have to be reviewed and changed if they do not provide an adequate level of security. In the interests of enhanced maritime security, additional responsibilities will have to be carried by the shipping and port industries and local agencies.

In implementing the amendments to SOLAS and the ISPS Code, any measures must be consistent with proper respect of fundamental rights and freedoms as set out in international instruments, particularly those relating to maritime workers and refugees. Furthermore, since the Convention on the Facilitation of Maritime Traffic, 1965, provides that foreign crew members shall be allowed ashore by the public authorities while the ship on which they arrive is in port, (provided that the formalities on arrival of the ship have been fulfilled and the public authorities have no reason to refuse permission to come ashore for reasons of public health, public safety or public order), maritime administrations and port authorities should pay due cognisance to the fact that ship's personnel live and work on the vessel and need shore leave and access to shore based seafarer welfare facilities, including medical care.³

The ISPS Code

The ISPS Code is divided into two parts – those that are mandatory and those that are recommendatory. The Code applies to passenger ships, cargo ships of 500 gross tonnage and upwards, engaged on international voyages, and port facilities serving such ships. States Parties shall decide the extent of application of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage. The Code does not apply to warships, naval auxiliaries or other ships owned or operated by Contracting Governments and used only on non-commercial service.

The functional requirements of the Code include gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments; requiring the maintenance of communication protocols for ships and port facilities; preventing unauthorized access to ships, port facilities and their restricted areas; preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities; providing means for raising the alarm in reaction to security threats or security incidents; requiring ship and port facility security plans based upon security assessments; and requiring training, drills and exercises to ensure familiarity with security plans and procedures.⁴

The Levels of Security

Three levels of threat have to be guarded against, requiring three levels of security. *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times. *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident. *Security level 3* means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.⁵

Company Security Officer

For a company operating ships, a Company Security Officer (CSO) has to be appointed by the company.⁶ This officer has to ensure that a ship security assessment is carried out and that a Ship Security Plan (SSP) is developed, submitted for approval, and thereafter implemented and maintained, and is responsible for liaison with port facility security officers and the ship security officer.

Ship Security Officer

Each ship is to have a special Ship Security Officer (SSO)⁷, accountable to the Master, and responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers. An SSP is to be developed for each ship to implement measures on board the ship to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

Port Facility Security Officer

In ports, a Port Facility Security Officer (PFSO)⁸ is to be appointed by the port authority to be responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan (PFSP) and for liaison with the SSOs and CSOs. The PFSP has to specify measures to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

The government will be responsible for designating which ports will be required to designate a PFSO and for approving the PFSP. This officer will be responsible for conducting the Port Facility Security Assessment and developing the PFSP. The government will be responsible for the issuance, if necessary, of a Declaration of Security. This will usually happen at the request of a ship that is operating at a higher security level than the port facility or another ship that the requesting ship is interfacing with. Alternatively, a Declaration of Security may be completed by the Master or the SSO on behalf of the ship.

Recognised Security Organisation

Governments are to set security levels taking into account: the degree that the threat information is credible; the degree that the threat information is corroborated; the degree that the threat information is specific or imminent; and the potential consequences of such a security incident. Governments may delegate port facility security functions to a Recognised Security Organization (RSO), with the exception of actually setting the applicable security level. Many Classification Societies are now holding themselves out to be RSOs, although the degree of knowledge and skill

of these organisations in the field of maritime security is unknown and unproven at the present time. There exists a potential conflict of interest when a Classification Society has been engaged to conduct a security assessment and/or develop a PFSP, and then the subsequent auditing of the effectiveness of such plan.

Ship Security Assessment Survey

Before an SSP can be developed, a Ship Security Assessment (SSA) has to be carried out by the CSO and/or with people with appropriate skills. This involves an on-scene security survey for the identification of existing security measures, procedures and operations; the identification and evaluation of key shipboard operations that it is important to protect; the identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and the identification of weaknesses, including human factors in the infrastructure, policies and procedures. The Ship Security Assessment must be documented, reviewed, accepted and retained by the company.

Ship Security Plan

When this Ship Security Assessment has been carried out, a Ship Security Plan (SSP) can be developed, to be approved by the maritime administration and to be carried on board the ship at all times. The plan must have responses for each of the three security levels. Where a recognised security organisation prepares a ship security assessment or a ship security plan, it must not be involved in the review and approval of the plan or in any amendments to that plan. The plan is to be written in the working language of the ship, or translated into English, French or Spanish.

The SSP is to address: (i) measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports from being taken on board the ship; (ii) the identification of the restricted areas and measures for the prevention of unauthorised access to them; (iii) measures for the prevention of unauthorised access to the ship; (iv) procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface; (v) procedures for responding to any security instructions given at security level 3; (vi) procedures for evacuation in case of security threats or breaches of security; (vii) duties of shipboard personnel who are assigned security responsibilities and of other shipboard personnel on security aspects; (viii) procedures for auditing the security activities; (ix) procedures for training, drills and exercises associated with the plan; (x) procedures for interfacing with port facility security activities; (xi) procedures for the periodic review of the plan and for updating; (xii) procedures for reporting security incidents; (xiii) identification of the ship security officer; (xiv) identification of the company security officer including 24-hour contact details; (xv) procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board; (xvi) frequency for testing or calibration of any security equipment provided on board; (xvii) identification of the locations where the ship security alert system activation points are provided; and (xviii) procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

International Ship Security Certificate

Once the SSP has been approved by the maritime administration, an International Ship Security Certificate (ISSC) will be issued, which is to be retained on board and available for inspection at all times, but shall be protected from unauthorized access or disclosure. SSPs are not subject to inspection by officers duly authorised by a Contracting Government to the SOLAS Convention to carry out control and compliance measures, unless these officers have clear grounds to believe that the ship is not in compliance and the only means to verify or rectify the non-compliance is to review the relevant requirements of the SSP. In this case, limited access to the specific sections of the plan relating to the non-compliance may be allowed, but only with the consent of the maritime administration of the Flag State or the Master.

The ISPS Code requires that some personnel receive training, and that drills and exercises be carried out to ensure the effective implementation of the SSP. The Code stipulates that shipboard personnel having specific security duties and responsibilities understand their responsibilities for ship security and have sufficient knowledge and ability to perform their assigned duties. Certain records have to be maintained, including training, drills and exercises; security threats and security incidents; breaches of security; changes in security level; communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been using; internal audits and reviews of security activities; and periodic reviews of the SSP.

Many of the security measures specified for ships are also applied to ports and port facilities. Certain activities are required for each of the three security levels including, at Security Level 1, controlling access, monitoring restricted areas and supervising the handling of cargo and ship's stores, as well as ensuring that security communication is readily available. Other measures are to be taken at the next two levels, as is described in Part B of the Code.

Port Facility Security Assessment

As with a ship, a Port Facility Security Assessment (PFSA) must be carried out before developing and updating the Port Facility Security Plan (PFSP). This assessment may be carried out by the Contracting Government or may be delegated to an RSO. In any event, the persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility. The assessment shall include: identification and evaluation of important assets and the infrastructure it is important to protect; identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures; identification, selection and prioritisation of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and identification of weaknesses, including human factors, in the infrastructure, policies and procedures. Such an assessment may cover more than one port facility if the operator, location, operation, equipment and design of these port facilities are similar.

Port Facility Security Plan

It is upon this PFSA the PFSP is based. Again the plan is to make provisions for the three security levels, and both the PFSA and PFSP shall be protected from unauthorised access or disclosure. Again, like the SSP, the PFSP may be prepared by a RSO, but those participating in the assessment or the development of the plan

should not be involved in any audit of its effectiveness. The PFSP should address: (i) measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship; (ii) measures designed to prevent unauthorised access to the port facility, to ships moored at the facility, and to restricted areas of the facility; (iii) procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface; (iv) procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3; (v) procedures for evacuation in case of security threats or breaches of security; (vi) duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects; (vii) procedures for interfacing with ship security activities; (viii) procedures for the periodic review of the plan and updating; (ix) procedures for reporting security incidents; (x) identification of the port facility security officer including 24-hour contact details; (xi) measures to ensure the security of the information contained in the plan; (xii) measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility; (xiii) procedures for auditing the port facility security plan; (xiv) procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and (xv) procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organisations.

Training, Drills and Certification

As with the CSO and the SSO, the port facility security personnel must have received training and fully understand their duties and responsibilities, as well as having a thorough knowledge of the port facility security. Drills and exercises shall be carried out as appropriate to ensure that the PFSA was valid and that the PFSP does what it is meant to do under the ISPS Code. The government in whose territory the port facility is located approves the PFSP. For ports, there is no equivalent to the ISSC that is issued after the initial or renewal verification, although a Statement of Compliance of a Port Facility might be deemed to be similar.

Implementation

The ISPS Code requires that a SSA be carried out from which a SSP can be developed. Similarly a PFSA is done prior to the development of a PFSP. This may be a difficult task for many Pacific Island countries with limited human and financial resources. The ISPS Code allows for the use of a RSO to assist in the preparation of a plan, but it also warns against the same persons or organisation carrying out the audit of an assessment or plan that they have been involved with. Furthermore, while some RSOs may be able to provide security experience, that experience may not be transferable to the Pacific region. The security issues of large ports or large cruise vessels are significantly different from those of ports like Honiara and Port Vila or from vessels operating inter-island passenger services or inter-regional freight services. As yet, international terrorists have not targeted Pacific Islands, although potential threats have been identified and the Bali bombings were not too far away geographically. Also, some Classification Societies have marketed themselves as RSOs for the purpose of identifying and resolving security risks, but their expertise is moot in this area at this time. An off-the-shelf copyrighted Ship Security Plan is actually being marketed on the Internet.

Although not much has been stated from official sources concerning the ramifications of failure to comply with the SOLAS Amendments and the ISPS Code, it is believed that some type of sanctions will be imposed on ships flying the flag of States that are not parties to SOLAS or have not applied the requirements of the ISPS Code to their ships. Ships that have not had an SSA or do not carry an SSP may have to proceed to an anchorage where an assessment of the threat that the ship presents to the security of the Coastal State is carried out. As a final resort, the ship may be denied access to a port in the State that is enforcing the provisions of SOLAS Chapter XI-2. This will obviously not go down well with shippers and consignees. Furthermore, a ship that has loaded, discharged or been in transit at a port that has not conducted a PFSA nor developed a PFSP may suffer the same fate as the ship without a SSP. In this case, shippers and consignees will be dissatisfied and may well ship with a company that does not sail to ports that do not subscribe to the international standards.

Self-help the Answer?

Many lessons can be missed by having someone else do things for you, especially when that requires local knowledge, some thought and/or discussion and the plan has to be implemented by local people, after the “experts” are long gone. Unfortunately, even consultants with the best of intentions unconsciously bring their experience, their values and their version of the solutions to a problem that could just as easily be resolved by local personnel and agencies, if provided with a bit of help to get started, a sounding board against which to bounce off ideas and a source from which to get some feedback periodically. In anticipation of this, the Regional Maritime Programme (RMP) of SPC has prepared some forms that enable port authorities to carry out their own port facility security assessment, and shipping companies to carry out their own ship security assessment survey. These forms are not necessarily all-encompassing, since many ports within the region differ one from another and may have aspects that need to be assessed differently from a security point of view. For example, a port facility may be laid out in such a manner that access control may be accomplished easily by the installation of a fence with a single gate between the highway and the port area, whereas another port facility may have numerous potential points of entry and egress, and different parts of the port may be separate one from another. However, all access must be controlled. Similarly, each ship is usually quite different from the next one, even if its length, tonnage and capacity are comparable. One may have a navigation bridge that is easy to secure, whilst another passenger ship may have difficulty, without major modifications, keeping unauthorised persons from restricted areas.

The Model Plans

Complementary to the security assessment forms are model PFSP and SSP. They have also been developed by the RMP of SPC. These are a reflection of the assessment forms. Like the assessment forms, they will have to be moulded to suit each specific situation. However, what they do is provide a model that can be followed. The models include much of the requirements of the amendments to Chapter XI of SOLAS and the ISPS Code, so that the plans follow the IMO measures and therefore should be more likely to be accepted by other ports and other maritime administrations. Local persons can use the assessment forms, as modified for their own situation, to carry out a security assessment of ports or ships without major intervention from outside consultants or experts. Having carried out the assessment,

the local administrators or managers can, by means of discussions with local stakeholders, develop a plan that will enhance port or ship security without overly disturbing operations. Then, after the local plan has been developed, implemented, tested, modified and validated, it can later be audited by RSOs who have had no prior involvement in that process and who are truly independent. These assessment forms and model plans can be found on the SPC website [http://www.spc.int/Maritime - Regional Maritime Programme](http://www.spc.int/Maritime-Regional-Maritime-Programme). The Regional Maritime Legal Advisor [peterh@spc.int] welcomes comments or suggestions for improvement.

Glossary

IMO.....	International Maritime Organization
AMSA.....	Australian Maritime Safety Authority
SPC	Secretariat of the Pacific Community
SUA Convention.....	Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988
SOLAS	International Convention for the Safety of Life at Sea, & SOLAS 1974.....1974;
AIS	Automatic Identification Systems
ISPS Code	International Code for the Security of Ships and Port Facilities
CSO.....	company security officer
SSO	ship security officer
PFSO.....	port facility security officer
SSA	ship security assessment
SSP.....	ship security plan
PFSA.....	port facility security assessment
PFSP.....	port facility security plan
RSO.....	recognised security organisation
ISSC	International Ship Security Certificate

¹ Peter Heathcote, B.Comm (cum laude), LL.B., M.B.A., Ph.D., FNI is the Regional Maritime Legal Advisor at the Secretariat of the Pacific Community, Private Mail Bag, Suva, Fiji Islands, (PeterH@spc.int) and provides maritime legal and policy advice to 14 Pacific Island countries.

² Four heavily armed Palestinian terrorists in October 1983 hijacked the Italian cruise ship *Achille Lauro*, carrying more than 400 passengers and crew, off Egypt. The hijackers demanded that Israel free 50 Palestinian prisoners. The terrorists killed a disabled American tourist, 69-year-old Leon Klinghoffer, and threw his body overboard with his wheelchair. Achille Lauro Hijacking Oct 7, 1985 <http://www.terrorismvictims.org/terrorists/achille-lauro.html>.

³IMO Conference of Contracting Governments to the International Convention of Safety of Live at Sea, 1974 – “Consideration and Adoption of the International Ship and Port Facility Security (ISPS) Code” - Document SOLAS/CONF.5/34 ANNEX 1 Page 4.

⁴ Ibid. SOLAS/CONF.5/34 ANNEX 1 Page 5.

⁵ Id. SOLAS/CONF.5/34 ANNEX 1 Page 6.

⁶ The duties and responsibilities of the CSO are outlined in section 11 of the ISPS Code.

⁷ The duties and responsibilities of the SSO are outlined in Section 12 of the ISPS Code.

⁸ The duties and responsibilities of the PSO are outlined in Section 17 of the ISPS Code.