ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ
στην
ΝΑΥΤ
ΛΙΑ

ΟΙ ΑΠΕΙΛΕΣ ΣΤΗ ΝΑΥΤΙΛΙΑΚΗ ΑΣΦΑΛΕΙΑ: ΠΕΙΡΑΤΕΙΑ, ΤΡΟΜΟΚΡΑΤΙΑ ΚΑΙ Ο ISPS CODE

Τόμκου Ιωάννα

Διπλωματική Εργασία
που υποβλήθηκε στο Τμήμα Ναυτιλιακών Σπουδών
του Πανεπιστημίου Πειραιώς ως μέρος των
απαιτήσεων για την απόκτηση του Μεταπτυχιακού
Διπλώματος Ειδίκευσης στην Ναυτιλία

Πειραιάς

Οκτώβριος 2009

Δήλωση Αυθεντικότητας

Δηλώνω οτι φέρω ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στην βάση των εξής παραγόντων: του σκοπού και χαρακτήρα της χρήσης (εμπορικός, μη κερδοσκοπικός ή εκπαιδευτικός), της φύσης του υλικού που χρησιμοποιώ (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες ή χάρτες), του ποσοστού και της σημαντικότητας του τμήματος που χρησιμοποιώ σε σχέση με το όλο κείμενο υπό copyright, και των πιθανών συνεπειών της χρήσης αυτής στην αγορά ή στη γενικότερη αξία του υπό copyright κειμένου.

Σελίδα Τριμελούς Εξεταστικής Επιτροπής

Η παρούσα Διπλωματική Εργασία εγκρίθηκε ομόφωνα από την Τριμελή Εξεταστική Επιτροπή που ορίσθηκε από τη ΓΣΕΣ του Τμήματος Ναυτιλιακών Σπουδών Πανεπιστημίου Πειραιώς σύμφωνα με τον Κανονισμό Λειτουργίας του Προγράμματος Μεταπτυχιακών Σπουδών στην Ναυτιλία.

Τα μέλη της Επιτροπής ήταν:

§ κ. Α. Γουλιέλμος – Επιβλέπον Καθηγητής

§ κ. Κ. Γκιζιάκης - Καθηγητής

§ κ. Ε. Τζαννάτος - Αναπληρωτής καθηγητής

Η έγκριση της Διπλωματική Εργασίας από το Τμήμα Ναυτιλιακών Σπουδών του Πανεπιστημίου Πειραιώς δεν υποδηλώνει αποδοχή των γνωμών του συγγραφέα.

Ευχαριστίες

Ευχαριστώ πρώτα τους γονείς μου που ότι είμαι «φταίνε» αυτοί για την υλική και πνευματική τους συμπαράσταση όλα αυτά τα χρόνια. Ευχαριστώ κατά δεύτερο τους καθηγητές μου που σχεδόν ότι ξέρω προέρχεται από αυτούς και για τις φιλότιμες προσπάθειές τους. Τέλος ευχαριστώ τον εαυτό μου που αν και εργαζόμενη κατάφερα να φέρω σε πέρας αυτές τις τόσο σημαντικές σπουδές και να πάρω αυτή την ειδίκευση που πιστεύω θα με κάνει καλύτερη στην εργασία μου αλλά και στην προσωπικότητά μου. Ειδικότερα θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Αλέξανδρο Γουλιέλμο για την συνεχή συμπαράστασή του και βοήθεια του, ως επίσης και τον καθηγητή μου κ. Κώστα Γκιζιάκη για τις πολύτιμες υποδείξεις του. Τέλος ευχαριστώ και τον Αναπληρωτή καθηγητή κ. Ερνέστο Τζαννάτο. Θα ήταν παράλειψή μου να μην ευχαριστήσω και την εταιρεία στην οποία εργάζομαι τα τελευταία έξι χρόνια, την Andriaki Shipping, στην οποία και εκπόνησα την εργασία μου καθώς και το τμήμα QSE της εταιρείας μου και ιδιαιτέρως την συνάδελφο κ. Παναγιώτα Χρυσάνθη - Deputy DPA -, που με βοήθησε παρέχοντας μου χρήσιμες πληροφορίες και κατευθύνσεις.

CONTENTS

Appendices:

List of tables:

ΠΕΡΙΛΗΨΗ

Οι βομβιστικές επιθέσεις στη Μαδρίτη (2004) και το Λονδίνο (2005) δείχνουν ότι, τα έθνη παραμένουν ευάλωτα απέναντι στους τρομοκράτες, παρά την αυξημένη ευαισθητοποίηση στα θέματα ασφάλειας μετά τις τρομοκρατικές επιθέσεις στις ΗΠΑ στις 11 Σεπτεμβρίου, 2001.

Υπάρχουν ομάδες που προσπαθούν να επιτύχουν τους στόχους τους μέσα από το χάος, τον εμφύλιο πόλεμο και τελικά ακόμη και την κατάρρευση των κοινωνιών. Γνωρίζουμε επίσης ότι ο φόβος επιτυγχάνεται εύκολα μέσω των επιθέσεων ευρείας κλίμακας σε υποδομές και άλλους οικονομικούς στόχους.

Παρόλο που κάθε οργάνωση μπορεί να διαφέρει ως προς τη φύση, τη δομή και τους στόχους της, κοινό χαρακτηριστικό τους είναι η ικανότητά τους να χτυπούν γρήγορα και τυχαία. Συνεπώς, είναι δύσκολο, αν όχι αδύνατο, να είναι κανείς σίγουρος πότε και πού θα συμβεί η επόμενη τρομοκρατική ενέργεια.

Ωστόσο, μετά τις επιθέσεις της $11^{ης}$ Σεπτεμβρίου, οι υπηρεσίες ασφάλειας συνειδητοποίησαν γρήγορα ότι η ναυτιλία, ο οδηγός του παγκόσμιου εμπορίου, αποτέλεσε πρωταρχικό στόχο για τους τρομοκράτες. Ως εκ τούτου, το 2002 ο Διεθνής Ναυτιλιακός Οργανισμός επισημοποίησε αυτές τις προσπάθειες με τον Κώδικα ISPS, ο οποίος τέθηκε σε ισχύ την 1η Ιουλίου, 2004.

Ο Κώδικας ISPS παρέχει ένα πλαίσιο για τις κυβερνήσεις, τους εθνικούς φορείς, τις τοπικές αρχές, τους φορείς εκμετάλλευσης πλοίων και λιμενικών εγκαταστάσεων για να συνεργαστούν και να λειτουργούν τα εγκεκριμένα σχέδια και τις διαδικασίες για να μπορούν να αντιμετωπίσουν αποτελεσματικά τις απειλές της ασφάλειας. Η ευθύνη για την προετοιμασία και τη θέση σε ισχύ αυτών των εγκεκριμένων σχεδίων ασφάλειας ανήκει στους αξιωματικούς ασφάλειας των πλοίων (SSO), τους Αξιωματικούς Ασφάλειας της εταιρείας (CSO) και τους υπαλλήλους ασφάλειας των Λιμενικών Εγκαταστάσεων (PFSO).

Αυτή η εργασία, ασχολείται κυρίως με τη φύση και την απειλή της πειρατείας στη

θάλασσα, η οποία είναι πολύ πιθανό να δοκιμάσει τα σχέδια και τις διαδικασίες ασφάλειας του πλοίου.

Το γεγονός ότι η πειρατεία εξακολουθεί να υπάρχει ακόμα και σήμερα μπορεί να προκαλεί σοκ σε πολλούς εκτός του κλάδου, που θεωρούν ότι αυτή υφίσταται αποκλειστικά στις ταινίες του Χόλυγουντ. Πράγματι, τα μέσα μαζικής ενημέρωσης τείνουν να υποτιμούν τα σύγχρονα κρούσματα πειρατείας. Αυτό άλλαξε όταν οι επιβάτες ενός κρουαζιερόπλοιου απειλήθηκαν από πειρατές στη Σομαλία το Νοέμβριο του 2005, και ζητήθηκε η έγκριση του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) για την εξεύρεση από τα Ηνωμένα Έθνη τρόπων για την προστασία των θαλάσσιων μεταφορών στον Ινδικό Ωκεανό.

Ωστόσο, μακριά από τα φώτα της δημοσιότητας, η αύξηση του αριθμού των ναυτικών που έχουν υποφέρει στα χέρια των πειρατών είναι τεράστια. Το Διεθνές Ναυτιλιακό Γραφείο (IMB), το οποίο ξεκίνησε την υποβολή εκθέσεων για τις επιθέσεις της πειρατείας το 1992, πιστεύει ότι ένα μεγάλο μέρος των κρουσμάτων δεν έχουν αναφερθεί ακόμη από τα θύματα.

Η πειρατεία είναι τόσο παλιά όσο και το θαλάσσιο εμπόριο και ο τρόπος οργάνωσης και ενέργειας τους παραμένουν τα ίδια σήμερα, όπως ήταν εκατοντάδες χρόνια πριν. η Πειρατεία συμβαίνει σε παγκόσμιο επίπεδο, όπου δηλαδή υπάρχουν πλοία. Το Θαλάσσιο εμπόριο δεν είχε ποτέ ένα τόσο ευρύ φάσμα από ότι έχει σήμερα, γεγονός που αντικατοπτρίζεται από την αύξηση των κρουσμάτων της πειρατείας.

Η πειρατεία καθοδηγείται από τη φτώχεια, την απληστία και την ευπάθεια των πλοίων στη θάλασσα.

Η σύγχρονη πειρατεία είναι βίαιη, αιματηρή και αδίστακτη, και πιο φοβερή για τα θύματα, επειδή οι πειρατές γνωρίζουν ότι αυτά είναι ανυπεράσπιστα χωρίς να έχουν κανέναν να μπορεί να τους βοηθήσει στη μέση της θάλασσας. Οι ναυτικοί είναι στην πραγματικότητα τα τέλεια θύματα.

Οι νόμοι, στον αντίποδα, ως προς την πειρατεία είναι ασαφείς στον ορισμό τους, ανεπαρκείς και δεν προστατεύουν τους ναυτικούς. Η ικανότητα των εθνών για την καταπολέμηση της πειρατείας είναι έως τώρα ελλιπής.

Λέξεις κλειδιά: Πειρατεία, Κώδικας ISPS, Αξιωματικός Ασφάλειας Πλοίου, Αξιωματικός Ασφάλειας Εταιρείας, Αξιωματικός Ασφάλειας Λιμενικής Εγκατάστασης

ABSTRACT

As the bombings in Madrid (2004) and London (2005) show, nations remain vulnerable to terrorists in spite of the heightened awareness and increased security efforts since the terrorist attacks on the US on 11th September, 2001.

Groups that try to achieve their goals through chaos, civil strife and ultimately even the collapse of societies, know that fear is easily achieved through wide scale attacks on infrastructures and other economic targets. And although each organization may differ in their nature, structure and aims, a common feature is their ability to strike quickly and randomly. It is therefore difficult, if not impossible, to be sure when and where a terrorist will strike next.

However, after the '9/11' attacks, security agencies quickly realized that shipping, a driver of global trade, was a prime target for terrorists. Therefore, in 2002 the International Maritime Organization formalized the 'International Ship and Port Facility Security (ISPS) Code', which came into force on 1st July, 2004.

The ISPS Code provides a framework for governments, national agencies, local administrations, ship operators and port facilities to work together and instigate approved plans and procedures that can effectively respond to security threats. The responsibility for preparing and putting into effect these approved security plans lies with Ship Security Officers (SSOs), Company Security Officers (CSOs) and Port Facility Security Officers (PFSOs).

This essay, deals primarily with the nature and threat of maritime terrorism and piracy, which is most likely to test the ship's security plans and procedures.

The fact that piracy exists today can still come as a shock to many outside the industry, confined as it is to history and Hollywood films. Indeed, reporting by the wider media has tended to trivialize modern incidents. This changed when cruise ship passengers were threatened by pirates off Somalia in November 2005, prompting the International Maritime Organization (IMO) to seek a United Nations Security Council resolution to protect shipping in the Indian Ocean

Yet away from the media glare, increasing numbers of ordinary seafarers have suffered at the hands of pirates. The International Maritime Bureau (IMB), which began reporting on piracy attacks in 1992, believes that a large proportion is not even reported by victims.

Piracy is as old as the maritime trade itself and its general tenets remain the same today as they did hundreds of years ago.

Piracy occurs world-wide, wherever there are ships trading. Maritime trade has never been more wide spread than it is today, a fact reflected by the growth in piracy.

Piracy is driven by poverty, greed and the vulnerability of ships at sea. Modern piracy is violent, bloody and ruthless, made all the more fearsome for victims because they know that they are defenceless, on their own, and with no help just over the horizon. They are in effect the perfect victims.

Laws are unclear in their definition, are inadequate and do not protect seafarers. The ability of nations to counter piracy is poor.

Key words: Piracy, ISPS Code, SSO, CSO, PFSO

INTRODUCTION: The Security of the Shipping Industry

Safety and Security are issues that any individual working in the Maritime industry must be familiar with. The transport of goods and passengers by sea is by nature vulnerable to a great number of risks: Perils of the sea, climatic change, natural disasters, accidents, (such as collisions between ships, fires and outbursts), acts of piracy, and even terrorist attacks.

For five thousands of years shipping played a leading part in the function of global trade and, as a matter of fact, it continues to do so and it is our opinions that it will do so in future till the end of this planet.

Nevertheless, its prestigious position as one of the great driving forces of the global economy has been “hit” several times in the past by maritime accidents and other tragic incidents which, apart from the obvious economic losses, in some occasions have had devastating effects. That is by claiming human lives and causing severe environmental pollution.

In today’s rapidly changing business environment, and with a world economy largely depending on Shipping for its prosperity, the need for the maritime industry to operate at the utmost efficiency and peace is urgent as ever. Thus, it comes as no surprise the fact that the issues related to Safety and Security in maritime transportation have in recent years become the subject of interest and thorough research and numerous studies by academics in a global scale.

In addition, state authorities from all over the world, as well as major maritime-related organizations, have during the last few years intensified their efforts in one major front. That is the process of formulating an effective regulatory framework that will promote Safety and Security in Shipping. The ultimate purpose of all the above is to promote efficiency in Shipping and to minimize -if not to eliminate- the risks for human losses, injuries and environmental pollution.

The organization that has a key role in the process described above is undoubtedly the International Maritime Organization[1] (IMO).

[1] It is an inter-governmental organization under the auspices of the United Nations (U.N.). It should be noted that the organization’s existence serves the purpose of promoting the collaboration between its member countries in the shipping area, the emphasis given on navigational issues. Its main

THE SCOPE OF THIS THESIS

We will focus on one of the most important Codes of the IMO: The International Ship and Port facility Security Code (ISPS Code). The examination of this Code forms the subject of this thesis together however with most other threats to Maritime Security and Safety like Piracy.

In recent years, after 2004, the ISPS Code has been placed in the centre of the academic debate with regard to the issue of Security, as mentioned. The vast majority of the interested parties (states, international organizations, shipping companies, and the academic community) agree that the ISPS code is setting efficient standards and promotes security at sea, the avoidance of human losses and injuries as far as the avoidance of pollution of the marine environment is concerned.

My selection of this specific subject is the result of a serious thought. The enhancement of security-related policies in the shipping industry has been so far the subject of thorough study and analysis in the maritime academic community, as mentioned. Yet, the developments that have taken place during the last few years within this framework are unprecedented and made the subject matter of immense importance for the shipping industry.

It should not be underestimated the fact that apart from the cost in human lives incidents that threat maritime security had many side effects also on tourism, a crucial sector that supports an economy.

For example:

- When terrorists, belonging to the Egyptian ‘Islamic Group’, attached cruise ships along the river Nile on four occasions between 1992 and 1994, tourists kept away from Egypt.
- In Somalia, when ‘warlords’ attached foreign ships sailing in the Gulf of Aden, vessels tried to keep away from the Somali coast.
- The attack on the French flagged tanker Limburg and the subsequent refusal of ships to dock in Yemeni ports was said to have cost Yemen

contribution towards the strategic goal of enhancing safety and security in shipping rests with the adoption of International Conventions (SOLAS) and the formulation of certain Codes that its member-states should comply with.

3.8 million dollars per month in lost revenue.

It seems crystal clear that there is an urgent need to intensify the efforts for amplification of the measures adopted by the shipping companies for maritime transportation with high standards of security. This dissertation as a result is placed within this framework.

CHAPTER 1: THE THREATS TO MARITIME INDUSTRY

1.1 Introduction

Nowadays, not even a week goes by, without the politicians or security experts to raise fears about new threats of *terrorism*. Security has never been taken more seriously than in the wake of the September 11th 2001 disaster.

The 11th September 2001 events have transformed most of the world's society more than anybody could have ever imagined. At the forefront of this transformation process is the maritime industry, which, perhaps, is experiencing as a result of terrorism more radical change than any other industry. And that is because most of the world's cargo is still and will be transported by ships.

Consequentially, shipping is a possible target for attacks aimed at the weakening of a well functioning economic system. Transportation is as valuable as the blood to a human being. In this connection, the vulnerability of *ports* is often criticized, especially considering the trend to mega- ports and mega-vessels.

Therefore, measures already adopted to combat violence and crime at sea needed to be reviewed internationally. On the other hand, not only the law regarding port and ship security had to be re-thought, but also regulations addressing cargo security in order to illuminate the whole chain involved in the act of transport.

1.2 The Security Problems in International Shipping

In order to be clear about how important is to focus on the security issue, we have to take a look at the risk factors that can potentially harm the international shipping. These are on one hand the *cargo* and the *vessels* themselves, and on the other hand the *people* and the *companies* associated with shipping.

1.2.1 The Seafarers. There are approximately more that one million officers and ratings manning the merchant fleet. Not all of them operate on international trading vessels, but a significant portion does. Seafarers have traditionally been granted relatively liberal *travel rights* by governments through non-immigrant crew list visas, or simply upon their presentation of their seafarer identity documents.

However, there is very little known about the men who operate the vessels. Any background checks prior to employment on board a ship is the legal responsibility of the flag state. One of the great attractions of "Flags of

Convenience" is that they allow vessels owners to crew the ship with foreign nationals as a means to control costs.

The employment of a large number of foreign nationals makes the implementation of enhanced reliability checks nearly impossible. This creates gaps that could be utilized by perpetrators in order to obtain employment with an overseas shipping company and thereby support their logistic operations.

1.2.2 The Vessels. The most obvious risk is the lack of security onboard the vessels themselves. There is a potential for an entire vessel to be used as a weapon such as the attack of port facilities or population centers adjacent to the ports, or the blocking of the access to ports by sinking vessels. On the other hand, previous incidents have tended to target the vessels rather than use them. It seems that modern day terrorism and piracy constitutes the two greater and most frequent threats to the security of a vessel. Thus we will now deal with Piracy.

CHAPTER 2: THE THREAT OF PIRACY ANALYZED

2.1 Piracy defined

Piracy, according to article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS), is defined as follows:

1. "Any illegal act of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship (or a private aircraft), and directed: (a) on the high seas, against another ship (or aircraft), or against persons or property on board such ship (or aircraft); (b) against a ship, (aircraft), persons or property in a place outside the jurisdiction of any State;

2. Any act of voluntary participation in the operation of a ship (or of an aircraft) with knowledge of facts making it a pirate ship (or aircraft).

3. Any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b).

2.2 The seaborne piracy

Seaborne piracy against transport vessels remains a significant issue, with estimated worldwide losses of US $13 to $16 billion per year, particularly in the waters between the Red sea and Indian Oceans, off the Somali coast, and also in the Strait of Malacca and Singapore.

These are used by over 50,000 commercial ships a year. A recent surge in piracy off the Somali coast spurred a multi-national effort led by the United States to patrol the waters near the Horn of Africa. While ships off the coasts of North Africa, Iran and the Mediterranean Sea are still assailed by pirates, the United States Navy and the U.S. Coast Guard have nearly eradicated piracy in U.S. waters and in the Caribbean Sea.

Modern pirates favor small boats and take advantage of the small number of crew members on modern cargo vessels. They also use large vessels to supply the smaller attack/boarding vessels. Modern pirates can be successful because a large amount of international commerce occurs via shipping.

Major shipping routes take cargo ships through narrow bodies of water, such as the Gulf of Aden and the Strait of Malacca, making them vulnerable to be overtaken and boarded by small motorboats. Other active areas include the South

China Sea and the Niger Delta.

As usage increases, many of these ships have to lower cruising speeds to allow for navigation and traffic control, making them prime targets for piracy. Small ships are also capable of disguising themselves as fishing vessels or cargo vessels, when not carrying out piracy in order to avoid or deceive inspectors.

Also, pirates often operate in regions of developing or struggling countries with smaller navies and large trade routes. Pirates sometimes evade capture by sailing into waters controlled by their pursuer's enemies.

With the end of the Cold War, navies have decreased size and patrol, and trade has increased, making organized piracy far easier. Modern pirates are sometimes linked with organized-crime syndicates, but often are parts of small individual groups. Pirate attack crews may consist of 4 to 10 sailors for going after a ship's safe (raiding) or up to 70 (depending entirely on the ships and the ships crew size) if the plan is to seize the whole vessel.

The International Maritime Bureau (IMB) maintains statistics regarding pirate attacks dating back to 1995.

Table 1: The results of Piracy on Crews, 2006-2007.

2006	2007
239 attacks against crew	263 attacks (+10%) 35% more gun attacks
77 crew members kidnapped	
188 crew members were taken as hostages	
17 crew members injured	64 crew members were injured
15 attacks resulted in murder	

Source: IMB.

The records indicate hostage-taking overwhelmingly dominates the types of violence against seafarers as shown in Table 1. In some cases, modern pirates are not interested in the cargo. They are mainly interested in taking the personal belongings of the crew and the contents of the ship's safe, which might contain large amounts of cash needed for payroll and port fees. In other cases, the pirates force the crew off the ship and then sail it to a port to be repainted and given a new identity through false papers often purchased from corrupt or complicit officials.

Modern piracy can also take place in conditions of political unrest. For example, following the U.S. withdrawal from Vietnam, Thai piracy was aimed at the many Vietnamese who took to boats to escape. Further, following the disintegration of the government of Somalia, ‘warlords’ in the region have attacked ships delivering UN food aid.

2.3 Armed suspected pirates in the Indian Ocean near Somalia

Environmental action groups such as ‘Sea Shepherd’ have been accused of engaging in piracy and terrorism when they sink ships by scuttling them, or ram them, and throw butyric acid (rancid butter) on their decks, and in one instance illegally boarding a Japanese whaling vessel. While only non-lethal weapons are used by the Sea Shepherd ships, their tactics and methods are considered acts of piracy.

The attack against the U.S. cruise ship the “Seabourn Spirit” offshore of Somalia in November 2005 is an example of the sophisticated pirates mariners face. The pirates carried out their attack more than 100 miles (160 km) offshore with speedboats launched from a larger mother ship. The attackers were armed with automatic firearms and an RPG.

Many nations forbid ships to enter their territorial waters or ports if the crew of the ships is armed in an effort to restrict possible piracy. Shipping companies sometimes hire private security guards.

Modern facets of piracy include the following acts:

Kidnapping people for ransoms. Murder.	Sabotage resulting in ship's subsequently sinking
Robbery.	Seizure of items or of he ship

In modern times, ships are hijacked for ***political reasons*** as well. The perpetrators of these acts could be described as pirates, but in English are usually termed "hijackers". An example is the hijacking of the Italian civilian passenger ship “Achille Lauro”, which is regarded as an act of piracy.

Modern pirates also use a great deal of technology[2].

2.4 Case- studies of recent incidents

- During the trouble years in Northern Ireland, two coaster ships were hijacked and sunk by the IRA in the span of one year, between February 1981 and February 1982.
- In October 1985, the cruise ship “Achille Lauro” was hijacked off the coast of Egypt by terrorists from the Palestine Liberation Organization. The terrorists demanded the release of PLO operatives imprisoned in Israel. Following the Israelis' refusal, the terrorists shot and killed disabled Jewish American tourist Leon Klinghoffer and dumped his body overboard.
- A collision between the container ship “Ocean Blessing” and the hijacked tanker “Nagasaki Spirit” occurred in the Malacca Straits at about 23:20 on 19 September 1992. Pirates had boarded on the “Nagasaki Spirit”, removed its captain from command, set the ship on autopilot and left with the ship's master for

[2] It has been reported that crimes of piracy have involved the use of mobile phones, Satellite phones, modern speedboats, Machetes, Combat knifes, assault rifles, shotguns, pistols, mounted machine guns, and even RPGs and grenade launchers.

ransom. The ship was left going at full speed with no one at the wheel. The collision and resulting fire took the lives of all sailors of “Ocean Blessing”; from “Nagasaki Spirit” there were only 2 survivors. The fire on “Nagasaki Spirit” lasted six days; the fire aboard the “Ocean Blessing” burned for six weeks.

- A Dutch motor tanker attacked outside the port of “All Saints Bay” in Brazil in November 1998. We had multiple injuries.

- The cargo ship “Chang Song”, taken over by pirates pretending customs officials in the South China Sea in 1998. Entire crew of 23 was killed[3]. A crackdown by the Chinese government resulted in the arrest of 38 pirates and the group's leader, a corrupt customs official, and 11 other pirates, who were executed.

- The New Zealand environmentalist, yachtsman and public figure Sir Peter Blake was killed by Brazilian pirates in 2001.

- Pirates boarded the supertanker “Dewi Madrim” in March 2003 in the Malacca Strait[4]. The American luxury liner “The Seabourn Spirit” was attacked by pirates in November 2005 off the Somalian coast. There was one injury to a crew member as he was hit by shrapnel.

- Pirates boarded the Danish bulk carrier “Danica White” in June 2007 near the coast of Somalia. USS “Carter Hall” tried to rescue the crew by firing several warning shots, but it wasn’t able to follow the ship into Somali waters.

- In April 2008 pirates seized control of the French luxury yacht “Le Ponant” carrying 30 crew members off the coast of Somalia. The captives were released after the payment of ransoms. The French military later captured certain of the pirates, with the support of the provisional Somali government.

- On June 2, 2008, the United Nations Security Council passed a resolution enabling the patrolling of Somali waters following the above and other incidents. The Security Council resolution provided permission for six months to

[3] Their bodies thrown overboard and six bodies were eventually recovered in fishing nets.

[4] Articles appeared in the Economist indicated that the pirates did not focus on robbing the crew or cargo, but instead focused on learning how to steer the ship and stole only manuals and technical information. The original incident report submitted to the IMO by the IMB would indicate these articles were incorrect and misleading. See also: the Letter to the Editor of Foreign Affairs.

states cooperating with Somalia's Transitional Federal Government to enter the country's territorial waters and use "all necessary means" to stop "piracy and armed robbery at sea, in a manner consistent with international law."

- Several more piracy incidents have occurred in 2008 including an Ukrainian ship, the “MV Faina”, containing arms consignment for Kenya, including tanks and other heavy weapons, which was possibly heading towards an area of Somalia controlled by the Islamic Courts Union (ICU) after its hijacking by pirates before anchoring off the Somali coast. The Somali pirates—in a standoff with US missile destroyer the “USS Howard”—asked for a $20 million ransom for the 20 crew members it held, shots were heard from the ship, supposedly because of a dispute between pirates who wanted to surrender and those who didn't.

- In a separate incident, occurring near the same time (late September to early October), an Iranian cargo ship, the “MV Iran Deyanatship”, departing from China, was boarded by pirates off Somalia. The ship's cargo was a matter of dispute, though some pirates have apparently sickened, lost hair, suffered burns, and even died while on the ship. Speculations of chemical or even radioactive contents have been made.

- On November 15, 2008, Somali pirates seized the supertanker “MV Sirius Star”, 450 miles off the coast of Kenya. The ship was carrying around $100 million worth of oil and had a 25-man crew. This marked the largest tonnage vessel ever seized by pirates.

- On April 8, 2009, Somali pirates briefly captured the “MV Maersk Alabama”, a 17,000-ton cargo ship containing emergency relief supplies destined for Kenya. It was the latest in a week-long series of attacks along the Somali coast, and the first of these attacks to target a U.S.-flagged vessel. The crew took back control of the ship although the Captain was taken by the escaping pirates to a lifeboat. On Sunday, April 12, 2009, Capt. Richard Phillips was rescued, reportedly in good condition, from his pirate captors who were shot dead by US Navy SEAL snipers. Vice Admiral William E. Gortney reported the rescue began when Commander Frank Castellano, captain of the Bainbridge, determined that Phillips' life was in imminent danger and ordered the action.

- In July 2009 Finnish-owned ship “MV Arctic Sea” sailing under Maltese flag was allegedly hijacked in the territorial waters of Sweden by a group of eight to ten pirates disguised as policemen. According to some sources, the pirates held the ship for 12 hours went through the cargo and later released the ship and the crew. However, an investigation into the incident is underway amidst speculation regarding the ship's actual cargo, allegations of cover-up by Russian authorities and Israeli involvement.

Authorities estimate that only between 50% to as low as 10% of pirate attacks are actually reported (so as not to increase insurance premiums).

2.5 Case-studies of Successful attempts against piracy

International ships equipped with helicopters patrol the waters where pirate activity has been reported, but the area is very large. Some ships are equipped with anti-piracy weaponry such as a sonic device that sends a sonic wave out to a directed target, creating a sound so powerful that it bursts the eardrums and shocks pirates, causing them to become disoriented enough to drop their weapons, while the vessel being pursued increases speed and engages in evasive maneuvering. The cases were: “MS Nautica”, December 2008; US-flagged “Maersk Alabama”, April 2009; Liberian-registered cargo ship, April 2009; US-flagged “MV Liberty Sun”, April 2009; The Marshall Islands-flagged Handy tanker “Magic”, April 2009.

1.6 The Legal authority about world prosecution[5]

There are legal barriers to prosecuting individuals captured in international waters. Countries are struggling to apply existing maritime law, international law, and their own laws, which limit them to having jurisdiction over their own citizens. According to piracy experts, the goal is to "deter and disrupt" pirate activity and

[5] A wartime activity similar to piracy involves disguised warships called “commerce raiders” or merchant raiders, which attack enemy shipping commerce, approaching by stealth and then opening fire. Commerce raiders operated successfully during the American Revolution. During the American Civil War, the Confederacy sent out several commerce raiders, the most famous of which was the “CSS Alabama”. During World War I and World War II, Germany also made use of these tactics, both in the Atlantic and Indian Oceans. Since commissioned naval vessels were openly used, these commerce raiders should not be considered even privateers, much less pirates—although the opposing combatants were vocal in denouncing them as such.

pirates are often detained, interrogated, disarmed, and released. With millions of dollars at stake, pirates have little incentive to stop.

Prosecutions are rare for several reasons. Modern laws against piracy are almost non-existent. For example, the Dutch are using a 17th-century law against "sea robbery" to prosecute. Warships that capture pirates have no jurisdiction to try them, and NATO does not have a detention policy in place. Prosecutors have a hard time assembling witnesses and finding translators, and countries are reluctant to imprison pirates because they would be saddled with them upon their release.

The nature of maritime piracy is evolving from the opportunistic petty criminal activity to the more sinister crime that is carefully planned by organizations willing to use extreme violence in pursuit of their booty. The protection offered to seafarers by UNCLOS III Convention proves inadequate and does not act as a deterrent for the pirates.

While the 1988 Rome Convention does provide those nations who wish to prosecute pirates a better chance of success, the problem lies not with what to do with pirates once they have been caught, but catching them in the first place. The statistics show that not only has the incidence of piracy sharply increased during the past ten years, but also the levels of violence associated with these crimes.

Ships are inherently vulnerable to attacks at sea. Pirates know that there is a low risk of being caught due to the remoteness of the areas in which the crimes take place. In the past, ships had been protected on the high seas by the state whose flag it flies. Today, many ships operate under 'flags of convenience'.

With decreasing naval budgets, many states do not have the resources required to offer suitable protection. This problem has been exacerbated by the expansion of the territorial waters of many states. Once again resources for policing the waters are scarce and the jurisdiction responsibilities of many of these territorial waters are disputed.

The IMB's Regional Piracy Centre (RPC) is the best example to date of a multilateral initiative working towards the eradication of piracy by helping to create this accurate picture. The IMB hopes that by increasing the quality of the intelligence given to policing authorities, the law enforcement agencies will be able to offer a timelier and more aggressive response to reported incidents, and consequently make more arrests and successful prosecutions.

There can be little doubt that modern-day maritime piracy is emerging as a complex security threat in the international system, yet until very recently there seems to be a certain reluctance to accept the true nature of the problem. But the solution will not be found by the maritime industry alone, as the inherent risks and costs of piracy appear to be accepted and absorbed by the shipping companies. The ultimate responsibility for combating piracy must lay predominantly with governments, both individually and collectively.

Together with assistance of international agencies such as the IMO and the 1MB, governments are the only organizations with the resources and motivation to combat the problem. There is sufficient evidence to suggest that much of the threat posed by today's piracy is orchestrated by major criminal organizations ashore, which not only finance the operations but market the loot as well.

Pirates are at their most vulnerable in their operating bases ashore and the desire to counter the problem must be driven politically. Targeting these land bases not only avoids the legal problems associated with maritime jurisdiction, but will also go a long way to driving pirates out of business and eradicating the problem.

Action must be taken before a major incident occurs such as an environmental disaster or the hijacking of a prestigious cruise ship. Such events would bring the problem to the full attention of the whole world, but the cost will be great.

CHAPTER 3: The Maritime Terrorism

3.1 Sea terrorism defined

The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group has offered the following definition for maritime terrorism:

"…the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities."

We can further define maritime terrorism as the use or threat of violence against a ship (civilian as well as military), its passengers or sailors, her cargo, a port facility, or if the purpose is solely a platform, for political ends.

The definition can be expanded to include the use of the maritime transportation system to smuggle terrorists or terrorist materials into the targeted country. Maritime terrorism is motivated by political goals beyond the immediate act of attacking a maritime target.

3.2 Analysis

Terrorist groups understand that the sea is central to a country's economy, trade and infrastructure. The effects caused by maritime terrorism, can be clearly seen in some of the following scenarios and incidents.

In all likelihood international terrorism will focus its subversive activities now and in the near future on more accessible maritime targets, commercial maritime lines of communication, ocean-going transport and passenger vessels. The aims are wide ranging and the consequences can be great.

Year 2000 – was the year of maritime terrorism. Despite earlier incidents, this vulnerability became obvious after a series of attacks between October and November, 2000. This was demonstrated most convincingly by the 12 October attack, organized by members of the terrorist organization Al-Qaeda, against the US Guided Missile Destroyer, "*USS Cole*". The fact that this successful attack was against a US warship illustrates strongly the vulnerability of maritime assets: major damage was sustained to the ship, 17 sailors were killed and 42 were injured when the demolition charge was prematurely detonated.

Western intelligence services determined that the success of the attack on the *USS Cole* also stimulated the interest of many terrorist groups in the technical means of conducting terrorist acts at sea, into which some groups invested considerable funds.

The real capabilities of maritime terrorists at both a tactical as well as a strategic level create a many-sided, threat to security on an international scale.

The intelligence and security services of a number of states made a serious analysis of the tactics and techniques of maritime terrorism. The three attacks by suicide volunteers at sea in under a month dispelled the doubts of many about the reality of the existence of such a threat.

Nevertheless, the main appropriations for ship self-defense weapons continued to be focused on countering traditional enemy threats from the air, sea and shore: air defense, anti-submarine warfare, space defense and missile defense the attack generated an immediate reaction by other terrorist groups in Asia and the Middle East and prompted them to organize other similar operations.

On 23rd October small craft with suicide volunteers from the ‘Liberation Tigers of Tamil Eelam (LTTE)’ organization destroyed one and damaged a second high-speed ferry in Sri Lanka. This was followed on 7th November by an attack on a small Israeli naval craft by fighters from the Palestinian ‘Hamas’ organization. The vessel was only slightly damaged because the demolition charge was prematurely detonated.

Western intelligence services determined that the success of the attack on the *“USS Cole”* also stimulated the interest of many terrorist groups in the technical means of conducting terrorist acts at sea, into which some groups invested considerable funds.

3.3 Piracy and terrorism

In its definition, the Council for Security Co-operation in the Asia-Pacific (CSCAP) Working Group on Maritime Co-operation, tried to distinguish, as well as examine, the link between maritime *terrorism* and *piracy*.

This is especially relevant to South-East Asia, Indonesia and the Philippines, two of the world's top pirate hotspots, both have terrorist organizations operating on their soil — “Jemaah Islamyiah”, the “Free Aceh Movement” and the “Abu Sayyaf Group” respectively. All three are believed to have maritime capability and utilize the expertise of local pirates, well versed in violent operations against shipping.

Yet despite piratical acts carried out by the “Tamil Tigers”, there is nevertheless some debate about the extent of the piracy/ terrorism crossover. In September 2005, for example, Indonesia’s Minister of Foreign Affairs, Hassan Wirajuda rejected a link outright: "We should not adopt alarmist views that somehow terrorists and sea robbers will join forces in wreaking havoc on the Straits of Malacca," he told a conference on maritime security. His reasoning was that the terrorist's aim is to halt world trade, something that would put the pirate out of business.

Mr. Wirajuda was right to the extent that pirates attack ships for gain rather than to further an ideological cause, although, as the bombing of “*Superferry 14*” shows this is not always clear-cut. His statement might better be understood when we consider the decision two months earlier by Lloyd's and the London insurance market's Joint War Committee to make the Straits of Malacca a high risk zone. This decision, based partly on the threat of terrorism, led to a sharp rise in insurance premiums for ships transiting the area and was widely condemned by the industry regional governments as stifling trade.

Pirate and terrorist motivation may differ but tactics in the seizure of ships and hostages certainly overlap. And in the context of South-East Asia, it is not unthinkable that terrorist groups might adopt techniques directly from pirates. Indeed, in Indonesia's piracy-ridden region of ‘Aceh’, it is quite conceivable that members of the ‘Free Aceh Movement’ could already be involved in pirate activities.

Whatever the debate, for those crew members or passengers unlucky enough to be attacked, it makes very little difference whether the armed men are terrorists, pirates or terrorists and pirates combined. What matters is that the SSO (ship security officer) has ensured that the ship's security procedures are ready for all eventualities

3.4 Terrorist organizations with a maritime capability

Abu Nidal. On 11th July 1988, three gunmen attacked passengers on a cruise ship, the “*City of Poros”*, in the Aegean, killing nine and wounding 98. The terrorists escaped aboard a waiting speedboat, and were not immediately identified.

A few days later, the police circulated photographs of three suspects, including a woman, who they said had been disguised as French tourists. The people in question, who had returned to France, immediately denied the allegation and were able to prove their innocence.

The Council on Foreign Relations and the MARKLE Foundation were certain that the terrorists were Palestinians. The attack coincided with the trial of Mohammed Rashid, who was charged and convicted of entering Greece with a forged passport. He claimed that his name was Mohammed Hamdan, but the police had his fingerprints, which showed that he had been convicted of smuggling hashish into Greece in 1973.

Just before the attack on the above cruise ship, a car exploded near the port where the "*City of Poros" was* to dock. Two passengers were killed, apparently the victims of their own bomb. One of them was thought to have been a senior member of Abu Nidal's team, Hejab Jaballah (using the name Samir Kadar), but the bodies were so severely mutilated that positive identification was impossible. Police were not even sure that there were only two bodies — there may have been three.

3.5 The Palestinian Liberation Organization

The Palestinian leader, Yasser Arafat, remained the most prominent Palestinian leader, dealing with the USSR, King Hussein of Jordan, President Mubarak of Egypt and, 'under the table', with the Israelis. Several members of his staff who were identified with the moderate faction were assassinated, and Arafat's own bodyguard, known as Force 17, was expanded: he was equally afraid of his Arab rivals as was of the Israelis.

Also, Arafat needed to demonstrate that he was still a guerrilla leader, and several groups in the PLO, including Force 17, were given the task of proving the point used the 'nom de guerre' Abu Jihad, called itself the 'Western Sector' because it was based in Tunis.

Its commandos were sent to ride Israel by sea. The first, a 28-man group aboard a small freighter, the *Atavirus,* was intercepted by the Israeli navy on 21 April 1985. The ship was sunk, 20 men were killed and the remainder captured. Despite that unpromising beginning, Force 17 tried the same tactic, sending a motor yacht, the "*Casselredit",* south from the Lebanon to raid Israel in May 1985. It too was intercepted and its eight-man crew, including Force 17's deputy commander, surrendered. The next Force 17 attempt - using another motor yacht, the "*Ganda",* sailing from Cyprus - was equally unsuccessful.

Events suddenly accelerated and on 25 September 1985, a three-man hit squad from Force 17 seized an Israeli yacht with three people on board, at a marina at Larnaca in Cyprus. First, they murdered a woman passenger, and then they demanded various concessions from Israel in exchange for their two remaining hostages. Eventually they murdered their prisoners and surrendered.

On 1st October, Israel retaliated with a long-range air raid against Yasser Arafat's headquarters in Tunis. The chairman was lucky to escape: 50 people, mostly PLO men, were killed. On the same day, the Italian cruise ship "*Achille Lauro"* sailed from Genoa.

3.5.1 The hijacking of the "*Achille Lauro*"

The well documented seizure of this ship was carried out by another one of Arafat's organizations, a faction led by yet another experienced terrorist leader, Abu Abbas. He booked four young men (the oldest was 20) on the ship and sent a relative to Italy to co-ordinate the operation. The relative was picked up by Italian police, and an Israeli raid on Tunis destroyed Abbas's communications system. The four men, who had smuggled large numbers of weapons on board, were left to their own devices. Abu Abbas claimed later that their mission was to wait until the cruise ship reached Ashdod, the main Mediterranean port in southern Israel, and then storm ashore and attack oil storage tanks.

The terrorists seized the ship on 7th October, after a sailor found their weapons. By this time the "*Achille Lauro" was* sailing along the coast of Egypt. Most of the passengers had left at Alexandria to visit the Pyramids and were to rejoin the ship at Port Said for the trip to Ashdod. However, there were still 427 passengers and a crew of 80 on the ship, and the four terrorists threatened them all with death. They demanded the release of 50 Palestinian prisoners in Israel.

When the Israelis refused, they murdered Leon Klinghoffer, a 69-year-old Jewish American tourist from New Jersey, who was confined to a wheelchair and ordered a sailor to throw his body overboard off the coast of Syria. In response, the Syrians refused to allow the ship to dock and it was forced to return to Port Said.

By then, Abu Abbas had reached Egypt and arranged with the Egyptians that the four terrorists would be allowed to go free if they surrendered the ship. The

PLO then claimed the credit for ending a crisis that it had itself begun.

Abu Abbas and the terrorists were put on an Egyptian airliner and flown out but the US Navy intercepted the plane over the Mediterranean and directed it to a NATO base in Sicily. But the Italians, who had not been warned, insisted on taking charge of the prisoners and subsequently released Abu Abbas and three of his assistants. The four terrorists were eventually taken into custody and tried for murder and piracy, resulting in sentence terms ranging from 15 to 30 years. The longest sentence was given to Klinghoffer's murderer. He escaped from jail in 1996, but was caught again in Spain.

3.6 The Irish Republican Army

For more than 30 years, Earl Mountbatten of Burma had spent every August in the Irish fishing village of Mullaghmore and was well liked by villagers. He never felt the need for a bodyguard.

Then in the morning of 27 August 1979, Mountbatten and members of his family set out for a day's fishing in their boat, "*Shadow V*". It had just left the harbor mouth when it was blown apart by an IRA bomb. Earl Mountbatten, aged 79, was killed instantly. His grandson, Nicholas, aged 14, and a 17 year old boatman also died in the blast.

Eyewitnesses described an explosion that blew the boat out of the water, smashing it into tiny pieces of wood. The IRA claimed responsibility for the execution of Lord Louis Mountbatten and said that the boat had been blown up by remote control. The bomb contained 50 pounds of explosives.

3.7 Euskadi Ta Askatasuna - ETA (Basque Homeland and Freedom)

In June 2001 Spanish police uncovered plans by Basque terrorists to plant a bomb on the car ferry from Santander, Spain to Plymouth, UK. The plot came to light after seven suspected ETA members were arrested. One was found to have plans for the "*Val de Loire*", which normally carries 2,140 passengers and 540 cars.

The ETA planned to alert authorities so that the ship to be evacuated before detonating the bomb in port. The man with the plans was imprisoned, along with another man believed to be a member of ETA's 'Blackbird' commando group.

ETA, which in 2006 declared a permanent ceasefire, clearly had the capability to carry out such an attack since earlier that year it had set off bombs at two Spanish resorts, apparently trying to damage the country's huge tourism industry. The ferry bombing would have been part of a larger violent campaign across the, north of Spain during the following tourist season.

3.8 Al-Qaeda

Osama Bin Laden's Al-Qaeda organization is considered to be a major maritime terrorist organization, although reports that there is a fleet of Al-Qaeda ships are treated with skepticism.

However, it was Al-Qaeda operatives that staged the spectacular waterborne suicide bombing of the *"USS Cole"* in October 2001, in the Yemeni port of Aden as well as the attack on the "*Limburg*". In addition, it has plotted several high profile maritime attacks that were foiled during their preparation phases. Additionally, Bin Laden's brother-in law reportedly operates a fishing boat business in Madagascar and Asia that might provide additional logistical support to future Al-Qaeda maritime operations.

After October 2000 attack on the "*USS Cole*", Al-Qaeda, through one of its Singapore satellite cells, again attempted to target US naval assets. This was foiled in December 2001 when the Singapore authorities detained 13 suspects, who were members of a clandestine "Jemaah Islamiyah" or Islamic Group cell. Although the main targets of this plot were the US Embassy and the residence of the US military in Singapore, the cell had reportedly planned to attack several US naval vessels moored off the coast of Singapore.

The Singapore plot was followed in May 2002 by the arrest in Morocco of three Saudi members of an Al-Qaeda cell that had planned to attack American and British naval ships in the Straits of Gibraltar. According to Moroccan authorities, the operatives had planned to sail from Ceuta and Melilla, the Spanish enclaves on Moroccan territory, using inflatable Zodiac speedboats loaded with explosives to crash into ships patrolling the straits.

3.9 Bin Laden's 'mystery ships'

In 2003 it was widely reported that US intelligence officials had identified a number of cargo freighters around the world, which they believed were controlled by Al-Qaeda or could be used by the terrorist network to ferry operatives, bombs, money or commodities around the world.

Osama bin Laden, Al-Qaeda's leader and his aides, is believed to have owned ships for years, some of which transported such commodities as cement and sesame seeds. One vessel is thought to have delivered the explosives that Al-Qaeda operatives used to bomb two US embassies in Africa in 1998.

Since September 2001, the US-maintained list of Al-Qaeda mystery ships has varied from as few as a dozen to as many as 50. Some of the vessels are said to be up to 130 meters in length so they do not need to refuel during long journeys and therefore are less likely to draw scrutiny. US officials do not know precisely how each of these "ships of concern" is being used, except that some are generating profits for Al-Qaeda.

The lack of concrete evidence since the statement was first made has led some to dismiss the reports as unsubstantiated stories. However, the nature of the shipping industry, with its lack of transparency means that the story should not be discounted lightly.

3.10 Al-Qaeda's changing strategy

Al-Qaeda has escalated its attempts to launch assaults at sea because it believes waterborne targets are more vulnerable. This is typical of the way Al-Qaeda constantly changes its operational methods, which leaves intelligence agencies struggling to predict where the next attack will be, what format will take and against what type of target.

More worrying fact is that Al-Qaeda no longer maintains complete control over terrorist groups affiliated with it, after Osama bin-Laden decreed that all such factions have complete autonomy to attack targets of western interest. This makes it much more likely that the maritime could become victim of Islamic fundamentalism.

Indeed, the possible scenario of Al-Qaeda-linked operatives infiltrating ships crews and seizing the vessel has led navy and coast guard officials to study student lists of hundreds of seaman's academies worldwide, taking the lesson from their trawl of flying schools after the World Trade Centre and Pentagon attacks.

Captured Al-Qaeda US efforts to track Al Qaeda’s activities at sea received a boost in November 2002 with the capture of Abd al-Rahim al-Nashiri, an alleged mastermind of Al-Qaeda’s nautical strategy who officials say is cooperating with US interrogators.

Intelligence agencies are now on the alert for signs that Al-Qaeda would use exotic craft to launch underwater attacks. Devices or operators may be delivered through the use of Swimmer Delivery Vehicles — mini submarines now available on the commercial market or small diver propulsion devices.

Captured Al-Qaeda operative Omar al-Faruq told interrogators that he planned SCUBA attacks on US warships in Indonesia. As a result of his confession US officials recently visited hundreds of SCUBA shops across the country asking about suspicious visitors.

3.11 Hezbollah

Hezbollah is an indigenous Lebanese group. Most of its terrorist operations are directed at Israel, its primary adversary and the majority of its operations take place on land. However, in the late 1990s, according to Singapore's Internal Security Department (ISD), a Hezbollah cell had plotted to bomb American and Israeli ships docked in Singapore. To accomplish this mission, Hezbollah operatives recruited five Singapore Muslims to assist with surveillance and logistics preparations.

Interestingly, Hezbollah's plan called for filling a small boat with explosives and ramming it into a ship in the Singapore Straits or in the harbor - the same modus operandi that Al-Qaeda later employed to bomb the “*USS Cole*” and the “*Limburg*”. According to Israeli intelligence, the similarity of the blueprints used by Hezbollah and Al-Qaeda was not 'coincidental' but part of a long standing operational co-operation. In fact, Hezbollah are believed to have provided Al-Qaeda with explosives training that may have played a role in Al-Qaeda’s 1998 bombings of the American embassies in East Africa and the “*USS Cole*” attack.

3.12 Abu Sayyaf Group

The Philippine radical Islamic “Abu Sayyaf Group (ASG)” uses boats to carry out some of its kidnapping and hijacking operations. Because of ASG's maritime warfare capability, Philippines maritime Special Forces are being trained by the US military to upgrade their counter-terrorism capability and it is hoped that the ASG capability will diminish accordingly.

The increasing effectiveness of the Philippines' Special Forces was demonstrated on 21st June, 2001, when they tracked down and killed Abu Sabaya, one of ASG's top leaders, and also killed two of his men as they were fleeing Mindanao Island in a boat. However, as the “*Superferry 14*” bombing of 2004 shows, ASG continues to attack soft civilian targets.

3.13 Liberation Tigers of Tamil Eelam (LTTE)

The largest number of terrorist acts at sea has been committed by the LTTE group fighting to establish an independent Tamil state in North Eastern Sri Lanka. As the acknowledged leader among Asiatic terrorist organizations, it created the most complete maritime component- essentially the world's largest non-state fleet, operating as two separate elements.

3.13.1 Sea Tigers

The Sea Tigers represent an amphibious group numbering 3,000-4,000 maritime terrorists, possessing capabilities for conducting terrorist acts and acts of piracy in territorial and coastal waters as well as on the high seas.

The Sea Tigers force is outfitted with the latest and best equipment; it makes its own floating mines and underwater Improvised Explosive Devices (IEDs), and has even managed to build a small submarine (subsequently captured by Indian security services). Experiments are presently being conducted with a torpedo controlled by a suicide volunteer.

The strength of the LTTE's naval capability is such that it is able to carry out engagements with the Sri Lankan Navy (SLIM). A favorite method includes the use small craft, often carrying suicide volunteers who carry out 'wolf pack' tactics. Operations are carried out on fast patrol vessels, gun boats and supply ships. For example, in February 1998, 20 Sea Tiger craft attacked eight SLN patrol ships, with up to 20 SLN sailors killed. These kinds of operations continue; in May 2006, 15 Sea Tigers craft, including suicide boats, attacked an SLN vessel that was transporting 710 soldiers. At least 15 SLN sailors and 30 Sea Tigers were reported to have been killed.

Another operation was the attempted destruction of a cargo transport carrying Israeli Kfir fighters to the port of Colombo. Luckily the ship put in for unloading a day earlier than planned and the suicide volunteers operation was disrupted. Indeed, as well as systematic guerrilla operations against the SLN and attacks against private fishing vessels, the Sea Tigers carry out acts of piracy against foreign commercial vessels.

3.13.2 Other activities

The Sea Tigers also perform other important functions such as transporting mercenaries and supplies in support of LTTE ground operations and monitoring their own economic zone. They meet their own ocean-going merchant vessels at the border of Sri Lankan territorial waters and escort them to points for offloading arms and other cargoes purchased abroad.

The ‘Marine Logistic Support Team’, special support flotilla of Mirage-class craft is used for this purpose. The vessels (length: 50 feet, beam: 16 feet) have a fiberglass hull, use four 250 hp diesel engines; are equipped with modern communications equipment and are armed with 50mm gun mounts, machine guns and other weapons. As with LTTE merchant vessels, they are also escorted by small craft (including those manned by suicide volunteers) from combat sub-units.

3.13.3 LTTE Merchant Fleet

The second element of the LTTE fleet, which brings together ocean-going merchant vessels, their own or chartered, is intended for the concealed movement of arms, mercenaries and drugs. It has its own command and control and communications system and operates independently of the Sea Tigers.

Vessels operated by companies specially created under the LITE 'cover' flying the flags of Panama, Honduras, Liberia, Cyprus, Greece, Malta and New

Zealand. The crews are Sri Lankan Tamils or foreigners and 90% of the time are used for transporting ordinary cargoes such as rice, flower, sugar, cement, fertilizers and timber.

The transport of legal cargo serves as cover for the delivery of arms, equipment, explosives and dual-purpose items. The West estimates that the overall volumes of military cargo shipments are the largest in the history of a guerrilla movement and terrorism.

4. Tactics and techniques of maritime terrorism

In the following section we examine operational side of maritime terrorism, the tactics they use and what makes them adopt those tactics.

4.1 Factors influencing the choice of tactics

The operating tactics of maritime terrorists against ships alongside and against vessels underway have their specific features and depend on many factors.

(1) Motivation and operational experience: The number of terrorist groups with the capability for committing subversive acts at sea are considered small, but the 2000 attack on the *“USS Cole”*, and subsequent attacks in the following weeks, demonstrated that the motivation and ability is there to be called upon quickly.

(2) Class and type of ship: Unlike their naval counterparts, merchant vessels, are vulnerable to terrorist attacks from shore and sea, and can be classed as soft targets.

(3) Importance and value of target: This is dependent on the effect to be achieved by the terrorist organization, for example the catastrophic loss of life or an ecological disaster.

(4) Security systems of the vessel and security systems of the harbor or port: These will focus the terrorist's tactics, which may vary from the use of ground teams trained to place explosive devices on ships, to the use of frogmen and the laying of sea mines.

The terrorists' technical outfitting ranges from modern skin-diving gear, diver propulsion vehicles and fast craft, to the most modern navigational systems for determining position (GPS). Because these are generally accessible technologies, it is rather difficult to monitor their acquisition; many modern technical means can be used, both for military as well as civilian purposes.

Equipment easily acquired on the commercial market helps to increase the effectiveness of the terrorist operations.

4.2 Explosive devices

If the harbor is unprotected, terrorists may well place an explosive device on the upper deck or any exposed areas of the ship chosen as the target. When the goal of a well-equipped group is to inflict maximum damage on the target, the explosive device could be placed on the ship's hull, below the waterline and in the vicinity of the engine compartment. For a terrorist organization that has operators with a SCUBA capability, this would be a relatively straightforward task.

Only a few terrorist groups possess the capability of minimizing their detection in order maximize the scale of damage inflicted. However, the very latest acquisitions in the equipment arsenal of some terrorist groups include special diving gear with a closed breathing cycle known as re-breather sets. Equipment such as LAR-V Closed Breathing Cycle Set effectively lowers the risk of the saboteur's detection due to the absence of exhaled air bubbles on the water's surface.

4.3 Use of submersibles

A terrorist diver carrying out an attack on a vessel would move to the target from the direction of the sea or shore, depending on the harbor’s geographic location and security system. When target approaches are guarded and it is a considerable distance away, the frogmen's air reserves may prove insufficient to execute the mission and withdraw to a safe distance; in this instance a diver propulsion vehicle could be used.

Although the finance, time and training are considerable for sub-surface attack, it is believed that terrorist groups are investing considerable funds in the purchase or construction of submersibles.

4.4 Use of speed, concealment and surprise

In an attack from the sea, factors of speed, concealment and surprise are achieved through the use of small, low craft, which have increased maneuverability and an insignificant radar signature. The security system even of a well-protected harbor can be breached with a simultaneous co-ordinate attack by several craft from different directions.

4.5 Deception

Commercial vessels have continued to be the preferred targets for terrorists, by using elements of camouflage, concealment and deception. For example, they have penetrated cruise ships in the guise of passengers, as in the case of the *“Achille Lauro”* in 1985.

Taking on the guise of coast guard or navy representatives is another tactic. Before attacking Indian fishing vessels, members of the Tamil Tigers organization would repaint their craft in the colors of the Sri Lankan patrol vessels and would also go aboard commercial vessels in the uniform of the national navy.

4.6 Remote control

Other innovative terror methods are also used. For example, members of the Basque Independence Organization - ETA, used a radio-controlled model boat filled with explosives to blow up a Spanish combatant ship.

4.7 Exchange of knowledge

A number of terrorist groups 'specialize' in the exchange of knowledge. For example, it is believed by western analysts that the Revolutionary Armed Forces of Columbia (FARC) obtained Naval mines with the help of corrupt foreign state officials.

Under present conditions, terrorist groups and organizations, both with land or maritime-based activities, actively exchange experience, technologies, ideas and methods of carrying out their actions. As a result of a shift in the 'centre of gravity' of international terrorism from the Near East to Afghanistan in Central Asia, opportunities opened up for closer co-ordination among extremist groups between the Middle East and the Asiatic-Pacific region.

5. Use of vessels to transport weapons

Several highly publicized incidents have occurred within the past several years involving terrorists' use of boats and ships to smuggle weapons. This trend is likely to escalate with the continuous need by terrorist groups to expand their arms and ammunition reserves.

5.1 The "*Santorini*" Incident

On 6 May 2001, the Israeli Navy captured "*Santorini",* a fishing vessel that was carrying weapons, including katyushas, anti-aircraft rockets, mortars of various calibers, and massive quantities of ammunition, in route from Lebanon to the Gaza Strip. The Israeli seizure resulted from a joint operation by the intelligence corps, the navy, and the air force. The Israeli military claimed that the weapons were intended for Palestinian terrorist groups for use against Israeli targets.

The ship had set off from the port of Tripoli in northern Lebanon and was headed in international waters for a 'rendezvous' point in the Gaza Strip. It was intercepted and detained off the northern Israel coast, but outside of Israeli territorial waters. Some of the weapons, which were carefully sealed in waterproof wrappings, had been packed into barrels and roped together.

Israeli newspapers have published two versions of how the arms were to be transported. According to one version, the airways to drop the barrels into the sea at a designated point off the Gaza coast where they would be retrieved by boats manned by Palestinian security services. According to the second version, the vessel was to be met by a fishing boat manned by Egyptian fishermen, who would then transfer the arms to a Palestinian fishing boat that would carry them to Gaza.

The "*Santorini",* which was manned by a crew of four Lebanese smugglers, was commissioned by a dissident Palestinian group led by Ahmed Jibril, the Popular Front for the Liberation of Palestine (PFLP)-General Command, a Damascus-based Marxist group that intended to step up attacks on Israel. The vessel's crew surrendered without any resistance and immediately told the Israeli naval officers what they were transporting. Following the vessel's capture, Jibril, speaking from his home in Damascus, Syria, said his group would continue smuggling weapons and munitions into Palestinian Authority-held areas.

Because katyushas have long been used by the Lebanese Hezbollah group, which had previously engaged in the smuggling of arms to Gaza by sea, Israeli analysts pointed to a possible connection between the PFLP-GC and Hezbollah. During the last decade, for example, Jibril had forged links with Iran and Islamic radicals, who would indicate that Iran, Hezbollah's patron, was most likely informed of this mission.

According to Israeli analysts, this was not the first time that this kind of method has been used. Reportedly in the past, similar shipments of arms in barrels had been unloaded onto beaches in Gaza and were hidden away in warehouses. In fact, the "*Santorini*" was apparently well known to Israeli security forces as a smugglers' vehicle in the 1980s and 1990s, and Israeli navy patrols had captured several of the crew on board had been apprehended. A further indication that the "*Santorini*" incident was not new was that the packing of the weapons was done in a professional manner by people used to dealing with arms who also appeared very familiar with Gaza arms smuggling operations.

5.2 "Karine A"

The "*Santorini*" affair was part of a larger, continuous maritime arms smuggling effort, which came to light in the early morning of 3 January 2002, when Israeli Defense Force (IDF) naval commandos seized the 4,000 tone "*Karine A*" general cargo ship in the Red Sea, some 300 nautical miles off the Israeli coast.

The ship was carrying 83 crates containing a variety of weaponry, including short and long range katyusha rockets, tank missiles, mortars, mines, explosives, sniper rifles, shotguns, plus other equipment, including Zodiac boats, cylinders, diving equipment and flotation containers for smuggling weapons. The operation's aim was to upgrade the Palestinian fighters' military capability with a huge quantity of long-range weaponry and explosives. According to Israeli authorities, the ship was part of a smuggling operation coordinated by the Hezbollah.

The ship's captain Omar Akkawi, a colonel in the Palestinian naval police, was arrested and said the shipment of arms was to be transferred to smaller boats near the Egyptian port of Alexandria. They would transfer again near the Gaza coast, where they would be picked up by Palestinian navy officers disguised as fishermen.

On 12th January 2002, in retaliation for "*Karine A*", Israeli military boats and divers attacked a Palestinian naval police base in Gaza City, destroying two patrol boats. One of the boats, named *“Jandala”,* was believed to be linked to the arms-smuggling operation. In fact, the *“Karine A”'s* captain and senior officer had reportedly previously served on the *“Jandala”.*

5.3 Recent piracy incidents

v “INDIAN OCEAN”: Bulk carrier reported suspicious approach 4 Jul 09 at 1800 UTC while underway in position 14:51.3N – 058:29.8E, approximately 220NM southeast of Sawqirah, Oman. The master of the vessel reported that one small boat approached the vessel during bad weather conditions with very rough seas and allegedly fired an RPG. The master conducted evasive maneuvers, increased speed, and managed to elude the boat. Office of Naval Intelligence (ONI) Comment: United Kingdom Maritime Trade Organization (UKMTO) contacted the master after the incident and was unable to confirm an attack. No weapons seen, no damage confirmed to date, and no attempt to board was noted (IMB, UKMTO, ONI).

v On Sunday, 31st May, early morning a British 115.000 tons tanker flying the flag of the Isle of Man was attacked by one skiff in position 1259N 04842E, right in the middle of the Transit Corridor. The eastbound ship was registered with the MSCHOA and reported immediately, while conducting countermeasures like evasive steering, which successfully avoided the ship being entered.

v 2nd May –Pirates hijacked a 69K DWT Bulk Carrier (Service Speed: Unknown, Freeboard: Unknown) in position 07°19’S 052°11’E. Although the ship operator had registered with MSCHOA website a vessel movement report had not been filed and UKMTO Dubai had not been receiving regular position, course and speed updates from the vessel. Little details are known about the hijacking but it suspected that the vessel was not keeping an adequate anti piracy watch and adopting adequate self protection measures.

v 7th May – A 3K DWT General Cargo ship (Speed: 10kts, Freeboard: 1.45m) was hijacked in approximate position 13°43’N 050°35’E. The vessel had been following recommended guidance during her Gulf of Aden transit and regularly reporting to UKMTO Dubai. However her relatively slow speed and low freeboard made her a vessel which pirates were able to board and gain control of before the nearest military unit was able to respond.

v Tanker (POLARIS) reported attempted boarding 11 Feb 09 at 1430 local time while underway in position 12:59N - 048:16E. Seven men in a white speedboat armed with automatic weapons and an RPG approached the tanker from the west. The captain sounded the alarm and alerted the crew, conducted evasive manoeuvres and activated SSAS. The tanker notified UKMTO, CMF, and naval warships in the area. The men in the speedboat used a portable ladder to try to climb onboard the tanker. The crew managed to detach the ladder before the men could climb onboard. After four attempts, the pirates aborted their attempt. A US warship in the area responded to the distress call and later arrested all seven pirates.

v Container ship (NEDLLOYD BARENTSZ) fired upon 13 Jan 09 at 0810 UTC while underway in position 12:24N - 044:57E. A small boat with 6 men onboard fired two RPGs at the vessel. The master increased speed and conducted evasive maneuvers. The boat followed for approximately 30 minutes with no further attacks reported. The Russian frigate (ADMIRAL VINOGRADOV) was in the vicinity and sent a helicopter to render assistance. The helicopter opened fire on the pirates' boat, wounding three, who were later captured and turned over to Yemeni authorities.

6. The Existing Law

Over the centuries, many attempts have been made to improve security in shipping. The measures originate in different approaches regarding the ports, the vessels, the seafarers and the cargo. New developments have always required changes in the international regime. However, arriving at practical solutions that do not impede the flow of goods and restrict international economic growth was and still is extremely difficult. In addition to the practical problems, there are legal difficulties resulting from the inadequacy of existing international instruments.

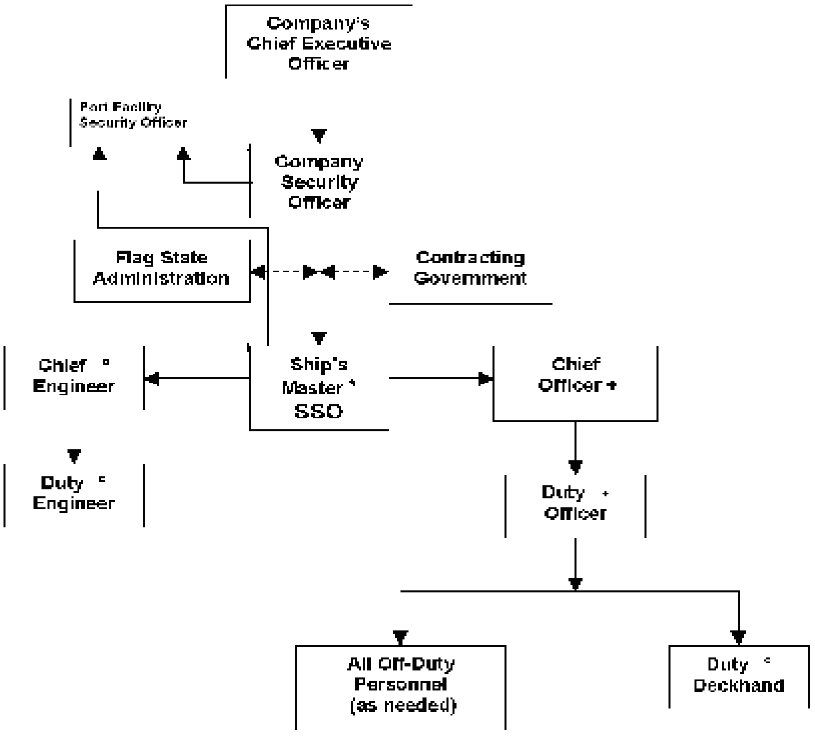
Over the years regional and international conventions were enacted that try to suppress or prevent security threats at sea. Nonetheless, these instruments are largely insufficient with respect to prevention of terrorism, because they have either attempted to fit terrorism within the scope of piracy or they have focused on the exertion of jurisdiction once an attack has occurred.

CHAPTER 4: The ISPS Code

4.1 Introduction

All the above reported cases of sea terrorism led to a Code development under the title of International Ship and Port Facility Security (ISPS). This is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Having come into force in July 2004, it prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to "detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade”.

Table 2: Security emergency response organization schematic diagram



* Master is the designated Ship Security Officer (SSO).
– Designated Security Team Leader, until relieved by SSO.
° Designated part of Security Patrol, when on duty.

4.2 History

The IMO stated that "The International Ship and Port Facility Security Code (ISPS Code) 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 in the wake of the 9/11/2001 attacks in the United States".

Development and implementation were speeded up drastically in reaction to the September 11th, 2001 attacks and the bombing of the French oil tanker “Limburg”. The U.S. Coast Guard, as the lead agency in the United States delegation to the “International Maritime Organization” (IMO), advocated for the measure. The Code was agreed at a meeting of the 108 signatories to the SOLAS convention in London in December 2002. The measures agreed under the Code were brought into force on July 1, 2004.

4.3 Scope

The Code is a two-part document describing minimum requirements for security of ships and ports. Part A provides mandatory requirements. Part B provides guidance for implementation.

In essence, the ISPS Code takes the approach that ensuring the security of ships and port facilities is basically a risk management activity and that to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. It is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities. The Code contains detailed security-related requirements for governments, port authorities and shipping companies in Part A, which is mandatory, in addition to a series of guidelines about how to meet these requirements in Part B, which is non-mandatory.

4.4 Application

The provisions of the Code apply to ships engaged on international voyages and consequently to port facilities serving such ships. *It does not,* however, apply to the whole port area, but only serves the ship/port interface. Measures for the remaining area were left to a joint work between the IMO and the ILO. The Code applies to passenger ships, cargo ships of 500 gross tonnage and upwards and mobile offshore drillings.

The Governments can, however, decide the extent of application to such ports which are used primarily for national trade and only occasionally are involved in international shipping. That gives on one hand a certain scope to states in order to maintain an undisturbed, seamless flow of goods within the country (noting that port regulation and security traditionally have been matters for state and local authorities), and on the other hand serves the international aim of these provisions. However, it could be used as a gap in the system if a state considers a port as not enough "international". Other ports would in that case have to categorize ships arriving from such ports into higher risk levels.

4.5 Responsibility of Contracting Governments

To begin the whole security process, each contracting government will conduct port facility assessments. For such security assessments different factors have to be considered:

- the degree that the threat information is credible;
- the degree the information is corroborated;
- the degree that the threat information is specific or imminent; and
- the potential consequences of such a security incident.

They must therefore identify and evaluate important assets and infrastructures that are critical to the port facility as well as those areas or structures that if damaged, could cause significant loss of life or damage to the port facility's economy or environment.

Furthermore, the actual threats must be identified in order to prioritize security measures. Finally, the assessment must address vulnerability of the port facility by identifying its weakness in physical security, structural integrity, protection systems, procedural policies, communication systems, transportation infrastructure, utilities, and other areas within a port that may be a likely target. Once these assessments have been completed, contracting governments can accurately evaluate risk. The next step is to set an appropriate security level in order to communicate the threat at a port facility or for a ship. Security levels 1, 2, and 3 correspond to normal, medium and high threat situation, respectively. The security level creates the link between the ship and the port facility, since it triggers the implementation of appropriate security measures for both.

Moreover, the governments have various responsibilities according to the Code, including the approval to the Ship Security Plans and relevant amendments to a previously approved plan, verification of the compliance of ships with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code (sec. 19.1.2), issuing the International Ship Security Certificate (sec. 19.2.2), ensuring the completion and approval of the Port Facility Plans and any subsequent amendments (sec. 16.2), and exercising control and compliance measures.

They are also responsible for communicating information to the International Maritime Organization and to the shipping and port industries. For all these purposes, governments can designate, or establish, Designated Authorities to undertake their security duties and allow Recognized Security Organizations to carry out certain work with respect to port facilities. That bears the risk of getting too much distance to official governmental work. However, the final decision on the acceptance and approval of this work should still be given by the government or authority.

4.6 Ship Security

Shipping companies will be required to designate a Company Security Officer for the company (sec. 11.1) and a *Ship Security Officer* for each of its ships (sec. 12.1). The Company Security Officer's duties and responsibilities include that a special Ship Security Assessment is properly carried out, that subsequently appropriate Ship Security Plans are prepared and submitted for approval by (or on behalf of) the administration, that security awareness and vigilance are enhanced, and that the personnel is adequately trained.

The abovementioned assessment resembles the assessment for the *port facilities*. The diverse weak links concerning the ship's security including human factors have to be considered. It is the foundation of the Ship Security Plan that indicates the operational and physical security measures the ship itself should take to ensure it always operates at security level 1. That means under the terms of the

Code that access to the ship is controlled, deck areas and areas around the ship are monitored, the handling of cargo and ship's stores is supervised, and the communication is readily available. Furthermore, the Plan should also show the additional, intensified security measures the ship itself can take to move to and operate at security level 2 and 3 when instructed to do so.

The *Ship Security Officer* is responsible for inspecting, maintaining, supervising and coordinating all security related aspects on board the ship. The Code could be interpreted as if the master of the ship is prevented from being the designated Ship Security Officer defining his special responsibilities, training etc. next to the master. However, that interpretation was not aimed and cannot be in the sense of an effective system. It has to be viewed in conjunction with chapter XI-2/8 SOLAS on "Master's discretion for ship safety and security", which makes it clear that the master has ultimate responsibility for safety and security, and could naturally also perform his duty as a Ship Security Officer. It is, however, for the national administration to decide if they wish to impose particular restrictions on who may serve as that special person on ships flying their flag.

The ships will have to carry an *International Ship Security Certificate* indicating that they comply with the security requirements. It will be issued by the flag state and lasts for five years. It can, however, cease to be valid, if a company assumes the responsibility for the operation of a ship not previously operated by that company, and upon transfer of the ship to a flag of another state.

When a ship is in a port or is proceeding to a port, the port's contracting government has the right, under the provisions of chapter XI-2/9 SOLAS, to exercise various control and compliance measures with respect to that ship. Therefore, the ship can be subject to port State control inspections. However, such inspections will normally not extend to examination of the Ship Security Plan itself expect in specific circumstances. The ship may, also, be subject to additional control measures if a contracting government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

4.7 Port Facility

Each contracting government has to ensure completion of a Port Facility

Security Assessment for each port facility within its territory that serves ships engaged on international voyages pursuant to sec. 15.2 ISPS Code. This assessment is fundamentally a risk analysis following the criteria of sec. 15.5 ISPS Code of all aspects of a port facility operation in order to determine which parts of it are more susceptible, or more likely, to be the subject of an attack. The security risk is evaluated in respect of a mutual connection of the threats coupled with the vulnerability of the target and the consequences of an attack.

On completion of the analysis, it will be possible to produce an overall assessment of the level of the risk. It will help to determine which port facilities are required to appoint a Port Facility Security Officer (sec. 17.1). Furthermore, the Port Facility Security Plan can be prepared out of this analysis. The plan should indicate – like a security plan on a ship – the measures the port facility should take to ensure that it always operates in the appropriate security levels. However, the Code was not intended to impede the international trade. Therefore sec. 14.1 ISPS Code clearly emphasizes that security measures and procedures shall be applied at the port facilities in such a manner as to cause minimum of interference with, or delay to, passengers, ships, ship's personnel and visitors, goods and services.

4.8 Enforcement

The system of the ISPS Code only works, if both ports and ships comply with the security procedures in order to adjust their security levels. If a ship does not comply with those requirements, it should not be issued with the International Ship Security Certificate.

As a consequence, contracting governments should direct those ships flying their flag to immediately discontinue operations until they have been issued with the required certificate. The ISPS Code does not provide a law enforcement provision for states. That will be left to domestic law. However, port state control will also drive compliance.

Ships are subject to controls when in a port of other contracting governments. If a vessel does not have a valid certificate, that ship may be detained in port until it gets a certificate. Of course, the port State has various other options available at its disposal, if there is no certificate. Regulation 9 of the new SOLAS Chapter XI-2 (XI-2/9) provides port states with the power to impose a range of control measures on foreign ships should they fail to prove their compliance with the maritime security regime or choose not to provide information that may be requested.

The authorities may curtail the operations of the ship, they may expel the ship from the port or they may refuse entry of the ship. Accordingly, the measures which are in place have been designed in such a way to ensure that those ships which do not have certificates find themselves out of the market in the shortest possible time. In addition, ships which call at port facilities that have failed to comply with the ISPS Code, although they may hold a valid Ship Security Certificate, may be faced with additional security requirements at subsequent ports of call, leading to delays and possible denial of port entry.

That could lead owners and charterers to the decision to instruct their ships not to proceed to port facilities which have not complied with the requirements of the ISPS Code, primarily, because of the problems such ships may encounter at subsequent ports of call.

4.9 Implementation

Since the ISPS Code is a part of the 1974 SOLAS Convention, it has to be implemented by all 146 contracting governments into national law. The Code came into effect on July 1st 2004. However, even if a contracting government does not adopt the rules into its own national legislation, the IMO would not be allowed to impose penalties. Nevertheless it is to be anticipated that the market forces and economic factors will drive compliance. In simple terms, if a state does not comply, ship operators will avoid its ports in order not to get refused or not to suffer from delays in destination ports because of security reservations. The other way around, shippers will avoid ships without a valid certification of its flag state for the same reasons.

CHAPTER 5: ASSESSMENT OF THE SECURITY

5.1 A Case of a piracy attack – roles and responsibilities

Basis of the Code requirements and in relation to a piracy attack, I will describe below (a) the responsibilities of the CSO and SSO, (b) the measures that have to be taken by SSO related to the attack, and (c) the issues that SSP and PFSP have to reflect in respect to such an attack.

5.1.1 Responsibilities of Company Security Officer (CSO) in relation to a piracy attack

Company security officer, as described by the code (Part A/2.1.7), is the person designated by the company responsible to ensure that ship security assessment is carried out and that ship's security plan is developed and implemented. CSO is also the liaison with port facility security officer and the ship security officer.

Depending on the size of the company fleet, the frequency of the calling ports and the security risks raised within vessel's trading area, CSO maybe responsible for one vessel specific and not for the whole fleet. Understanding that cruise vessels have a frequent interaction with the port facilities and a considerable number of passengers accessing the vessel, CSO has more security concerns compare to these he has on a cargo vessel.

In the case of a piracy attack, this is a security incident resulted to the transportation system disruption and individual injuries. Assuming that a security alert had been activated by the vessel and CSO had been alerted that the ship was in security danger, and thus CSO was responsible to:

- Contact with the vessel on a confidential way by using a "code phrase or word" and get as many information as possible in respect to the current situation on board.

- Upon he contacted with the vessel but also even if he hadn't managed to do so, he had to contact with the Security point of contact of vessel's flag and of the port where the incident took place and report the incident

- Coordinate all necessary actions required to send assistance to the vessel if required

- Report the incident to the reporting stations in order all ships in vicinity to be notified accordingly

Upon security integrity of the vessel had been restored, and the vessel sailed for the next port to disembark the passengers, CSO had to request from SSO to conduct a ship security assessment to ensure vessel's security integrity and to send a complete report of the incident to CSO and flag administration.

At next calling port CSO had to visit the vessel and conduct a ship security assessment in order to:

- Identify the exact threats that have encountered by the ship basis the incident taken place
- Ensure the Ship Security Plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- Conduct an internal audit and review of security activities
- Arrange for any subsequent verifications of the ship by the Administration or Recognized security Organization (RSO) if required after the incident

5.1.2 Responsibilities of Company Security Officer (SSO) in relation to the attack

In this event of a security incident SSO has to determine what actions are necessary to ensure the safety of the crew and of the ship and protect the environment. In communication with Master is responsible to order the actions to be taken by the ship's Security Team in which Ship Security Officer will act as the Team Leader, unless an alternate is designated depending the circumstances (if SSO is unavailable and/or injured etc.). SSO has to coordinate all the necessary actions required on board to restore vessel's security integrity.

In the event that emergency assistance is needed from local law enforcement, this request will be made by the SSO, in communication with CSO, with the facility or port, ship's agent, or directly to the local law enforcement agency, whichever is faster. In any event, the facility and port has to be advised of all significant security incidents. Reports of security incidents and suspicious activity have to be entered into the ship's log.

Ship Security Officer is responsible to conduct an investigation of all security breaches taken place. A report detailing the security breach, results of the investigation and corrective action recommended or taken should be prepared by the SSO and submitted to Company Security Officer. An example of this report is given in Appendix I. SSO is also responsible to provide all the necessary information in relation to the attack to the PFSO of the next calling port.

Further to the above, SSO is responsible to:

- Conduct security inspection of the ship to ensure that security equipment onboard the ship is properly operated, tested, calibrated and maintained.
- Maintain and supervise implementation of the Ship Security Plan, including any amendments to the plan.
- Enhance security awareness and vigilance on board ship.
- Ensure that adequate training has been provided to shipboard personnel, as appropriate.
- Conduct security survey of the port.
- Ensure consistency between security requirements and the proper treatment of ship personnel affected by those requirements, and,
- Review and complete a Declaration of Security agreement.

Provide security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

5.1.3 Ship Security Plan – Vessel’s reaction to a heightened risk of attack

Further to above, another crucial point is raised in respect to SSP Content. The ship security plan has to clearly define the actions to be taken by the vessel, depending on the trading area and the security level maintained in these areas.

Due to the severity of the consequences of a potential attack to the vessel, SSP has to reflect the procedures to be followed and the action to be taken by SSO, when vessel sails in an area with heightened risk of attack.

SSP has to reflect the procedures to respond to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface. In readiness condition, SSP reflect the following actions that are required to be taken by the vessel to:

- § Ensure the performance of all ship security duties.
- § Monitor access to the ship.
- § Monitor the deck areas and areas surrounding the ship.
- § Monitor the embarkation of persons and their carry-on items.
- § Supervise the handling of cargo and ship's stores.
- § Ensure that port-specific security communication is readily available.

When entering a port, a ship is required to act upon the security level set by the Contracting Government. A ship, Company or Administration, may choose a higher security level than recommended by the Port Facility Security Officer.

SSP plan has to clearly reflect that SSO cannot change the security level on board, but he (she) can increase the security measures taken by the vessel corresponding to a higher security level in order to ensure vessel's security integrity. In heightened risk areas and under threat alters, the SSP should leave at SSO discretion to take actions additional to these included in the SSP to minimize the risk of attack.

In heightened risk areas, SSP has to instruct SSO and crew to implement the highest level of preventive and protective security measures identified in this plan. Following general measures need to be reflected in the plan on how to:

- Post personnel to continuously guard critical restricted areas, such as the bridge and engine room.
- Increase the frequency of or establish continuous Security Patrols.
- Place the Security Team on alert.
- Coordinate enhanced security measures with the port and facility.
- To keep security equipment in readiness for use (long range acoustic device (LRAD) (etc).
- Use of armed security personnel to control access to the ship and to

deter to the maximum extent practical a Transportation Security Incident (TSI), or,

- Screening the ship for the presence of dangerous substances and/or devices underwater, or other threats.

Specific security duties and procedures have to describe in the plan to prevent an attack and to respond to an attack. A checklist has to include in the SSP detailing the actions to be taken if an attack takes place. The actions to be taken vary if the vessel just transits an area or approach a facility in the area. This checklist has to include the objectives of the response, the tactics to be followed, the actions follow up and the notifications required as follows below. The checklist may have the follow structure:

Table 3 - Unauthorized Boarding (Piracy)-Checklist

Objectives	Protect Human Life and Welfare. Protect Property and Environment.

Tactics	When approaching or berthing at a port or facility in a high-risk area: Minimize access points preferably to a single controlled gangway or ship's side companion way. Keep emergency ladders clear of the water; raise and stow pilot ladders immediately after use. Provide additional security officers at access points if a threat warrants the response. Establish perimeter security measures, such as weather deck and ship side lighting, deck and jetty patrols. Search all visitors and escort them while on board. Keep small craft in the vicinity under constant surveillance. Carefully control documents containing information about the cargo or ship's itinerary. Conduct a search of the ship and secure all doors and other access points. Brief crew members on the risks of being attacked by pirates or armed bandits. Secure the bridge, engine room, steering gear compartments, officers' cabins, and crew accommodations. Carefully plan any response to an apparent attack and ensure the crew is appropriately trained. Consider delaying ship arrival if there is a high threat from piracy at port and if a berth is not immediately available to minimize the Ship's vulnerability while in queue.	
Initial Actions	Activate Alarms.	
	Contact Local Emergency Services.	
	Contact Company Security Officer	
Life Safety	Evacuation Yes p No	Evacuation Means Lifeboat p Other:__________________

	Muster/Accountability Status: Missing:	Last Known Locations: Confirmed MOB:	
Noti/ns	Name/Title	Contact Numbers	Note/Tim Notified

5.1.4 Security measures to be taken prior –during and after the attack, by SSO and crew

As it was described above, there are certain actions that are reflected to the SSP in respect to the actions must be taken by the vessel when sailing in heightened risk areas. SSO is responsible to coordinate the vessel's readiness prior an incident and vessel's response during an incident and after this.

Specific measures shall be employed before, during and after the attack. It is important to underling that SSO has always to bear in mind that Master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request assistance of the Company or any Contracting Government, as may be necessary.

The Master shall not be constrained from taking or executing any decision that, in the professional judgment of the master, is necessary to maintain the safety and security of the ship.

If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the Master shall give effects to those requirements necessary to maintain the safety of the ship. In such cases, the Master implements temporary securities measures and inform the Administration, Company, and, if appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures shall, to the highest possible degree, be commensurate with the prevailing security level.

Even at Security Level 3 (as in the case of the attack)the Master has to seek clarification or amendment of instructions issued by those responding to security incident or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

5.1.5 Measures to be taken prior an attack

As it has been mentioned above, SSP reflects specific actions and measures than should be taken by SSO and crew to prevent a potential attack, when sailing in heightened risk areas. Further to these actions, prior vessel enters in a heightened risk area where an attack is possible to take place following additional measures have to be considered:

- SSO has to assign one of the qualified G/O other than the Master to be called upon to be the Designated General Operator. In addition to the Navigating Officer, it is advisable to have a duly qualified dedicated G/O to perform the GMDSS Watch, to ensure the ship's bridge is adequately manned when transiting potentially hazardous waters.

- Prior to entering areas where attacks have occurred or where intelligence indicates attacks may occur, General Operator should practice and perfect pertinent radio operational procedures and ensure all transmitters, including satellite earth stations are fully operational and available for immediate use on distress and security frequencies.

- Where an INMARSAT ship earth station is provided it is appropriate to draft and store "standard messages" for ready use in an emergency. Master should ensure that all procedures to generate a distress alert on any communication equipment are clearly marked on, or near, the equipment and all appropriate crewmembers briefed on their operation.

- A special Code for piracy/armed robbery/attack has to be available for use on digital selective calling (DSC) equipment. DSC equipment shall be modified to incorporate this facility. The Company is responsible for making sure the Company Security Officer and the Ship Security Officer have communicated with Coast State and Port Authorities to develop the list of contacts needed to establish a plan that works.

- The Master and all Radio Operators should be aware that potential attackers might be monitoring ship to shore communications and using intercepted information to select targets. When transmitting information regarding cargo, valuables and the status of ship’s stores, caution is advised.

- If a suspicious ship at sea approaches in a threatening manner **Master has to:**

Ø Increase speed and alter course if safe to do so.

Ø Do not allow the ship to come alongside; do not respond to messages by radio, light, or hailing.

Ø Note details of the threatening ship and video or photograph the ship if possible.

Ø At night, switch off the weather deck lighting; direct searchlights at the approaching ship.

Ø Keep personnel clear of the weather deck.

SSO shall make sure that the appropriate Contracting Government authorities are contacted to report any suspicious movements, which may result in imminent attack, and Piracy and Armed Robbery Increase the Restricted areas on board as required by the circumstances.

In addition, if the Master believes the other ship’s movement constitutes a direct threat to his ship or a danger to navigation in general, he shall consider sending an “All Stations (CQ) “danger message” as well as advising the appropriate Contracting Government authority. A danger message should be transmitted in plain language on a VHF working frequency following an announcement on VHF Channel 16 and or transmission of a DSC Call on VHF Channel 70 using the “safety” priority. All such messages shall be preceded by the safety signal (SECURITE).

The Ship Security Officer has to alert ship personnel of changes in security conditions on board the ship.

5.1.6 Measures to be taken during the attack

Specific scenario-based contingency plans and standard operating procedures may be developed to address identified threats

When the Master has concluded that the safety of the ship is threatened, he shall:

- Activate the Security Alert.
- Notify the cognizant Contracting Government authority and if considered appropriate authorize a broadcast of an “All Stations” “Urgency Message” on VHF Channel 16, 2182 kHz or any other radio communications he considers appropriate (e.g. INMARSAT). Such messages shall be preceded by the appropriate Urgency Signal (PAN PAN) and or a DSC call on VHF Channel 70 and /or 2187.5 kHz.

When an attack has occurred and in the opinion of the crew and of the ship are in grave danger requiring immediate assistance, the Master shall authorize the broadcast of a “Distress” message be preceded by the appropriate Distress alerts (Mayday, SOS, DSC, etc..) using the radio equipment most appropriate for the area taking into account the GMDSS Designation. The appropriate Contracting Government authority shall acknowledge receipt of the message and attempt to establish communications.

SSO has to alert security team and coordinate the response to the attack by using all the available means on board to prevent passengers and ship’s safety. In the measures he has to take following are included:

- Repelling boarders.
- Securing all access to the ship to prevent intrusion.
- Securing non-critical operations to focus attention on response.
- Alerting ship of an incident.
- Rendering assistance to a nearby ship undergoing an unlawful act.
- Screening the underwater hull or search the ship in response to bomb threats.
- Specifying the kind of communications to use in the event of a breach of security, and unlawful act, or other emergency.
- SSO if circumstances allowing him at the time, he has to report immediately the Security Incident to CSO and local authorities.

5.1.7 Measures to be taken after the attack

After the attack, and depending on the course of the events, SSO has to restore vessel’s security integrity to prevent further breaches. Necessary notifications have to be sent to CSO, Port Authorities, ships in vicinity and Flag administration.

Ship Security Officer should conduct an investigation of the attack. A report detailing the security breach, results of the investigation and corrective action recommended or taken should be prepared and submitted to Company Security Officer.

SSO has to conduct a ship security assessment to ensure that the current SSP is implemented and to review the security activities in order to conclude if SSP need to be amended to accommodate new security measures to avoid re occurrence of an attack.

SSO has to review crew response to the attack and identify new training needs a detailed entry describing the attack and the security measures has to be made in ship’s security log and appropriate records have to be kept available for inspection whenever it is necessary.

5.1.8 Next calling port - Port Facility Security Plan requirements

The next port facility should have a developed Port Facility security plan adequate for the ship/port interface as required by ISPC. The plan should to reflect the procedures to be followed when a vessel attacked by pirates proceeds to the port. It is at the port facility decision to restrict the entrance of any vessel that has been recently attacked by pirates. On the other hand such a decision would create commercial restrictions to the port.

A vessel on her arrival to a next port of call, she will have a higher security level because of the attack. Port facility security plan may require in this case that SSO has to contact well in advance with the PFSO and send his a report of the security incident details.

PFSP should instruct PFSO to complete a Declaration of Security (DoS). The DoS shall address the security requirements that could be shared between the port facility and the ship and shall state the responsibility for each.

PFSP should reflect that a DoS is requested when,

- the ship has a higher security level than the port facility,
- the ship activities pose a higher risk to persons, property or the environment for reasons specific to that ship, including her cargo or passengers or the circumstances at the port facility or a combination of these factors.

The PFSP will state that PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking passengers.

The plan should also reflect that the vessel upon arrival should restrict any movement of the passengers and crew until a port facility security team board the vessel and conduct a security assessment to ensure that it is safe for the vessel and the port to remain in the port. This assessment may be required to be conducted on a mile zone away from the berth facility.

CONCLUSIONS

When CSO, SSO implement their responsibilities and when the on board crew is trained to respond to a security incident, the consequences may not be as severe as it could be for the vessel and the passengers.

In this context, SSP has to reflect all the security issues that may arise during vessel’s trading and especially in heightened risk areas. SSO and crew has to be familiar with the procedures needed to be taken to prevent an attack, to respond to an incident and to follow up the necessary notifications.

Port facility on the other hand, needs to have an established Port Facility Security Plan detailing the measures to be taken when a vessel which was attacked calling the port. In any case measures have to be taken from the port to prevent the port itself and the berthed vessels from posing them in a security breach.

REFERENCES – BIBLIOGRAPHY

1. International Ship & Port Facility Security Code & SOLAS amendments 2006/Chapter V &XI.

2. Cruise Critic –Review and news (http://www.cruisecritic.com/news/news.cfm?ID=1445, last accessed on 07/09/09)

3. BIMCO Publication– Maritime Security: Guidance for Ship Operators on the IMO International Ship and Port Facility Security (ISPS) Code”, 1st Edition 2003.

4. “Pirates and Armed Robbers: Guidelines on Prevention for Masters and Ship Security Officers, 4th Edition 2004 (ICS/ISF).

5. ICS Model Ship Security Plan- 1st edition 2003 (ICS).

6. Maritime Security (http://www.imo.org/Newsroom/mainframe.asp?topic_id=551 last accessed on 12/09/09)

7. MSC 75/24 issued on 29 May 2002 (Report of the Maritime Safety Committee on its Seventy –Fifth session).

8. OCIMF Survival Craft – A Seafarers Guide, Witherbys Publishing p 3-42

9. Κώδικας ISPS 2003, εκδόσεις Εμμανουήλ Ν. Σταυριδάκη

10. Steven Jones (2006). Maritime Security – A Practical Guide. The Nautical Institute

APPENDIX

SSP OF A BULK CARRIER

SHIP SECURITY PLAN. IN CONFORMANCE WITH

IMO - INTERNATIONAL SHIP & PORT SECURITY (ISPS) CODE

M.V X

IMO NO: XX

DISTRIBUTION LIST

This copy of the *Ship Security Plan* is written in the working language of ships crew (English) and it is distributed as follow:

Copy No	Description of Plan	Holder
SSP/01	Hard copy –Controlled pages	SSO of MV X
SSP/02	Electronic Format [floppy disk]	CSOs
SSP/03	Hard copy	Greek Ministry of MM [DEDAPLE]

All above copies of the plan are confidential and kept under holder's custody.

PREFACE - RECORD OF CHANGE: this copy of the *Ship Security Plan* was prepared on xxx and is copy # initial. All pages of the plan are marked "controlled" verifying that the whole manual is under CSO control and under CEO approval.

This plan will be reviewed at intervals to ensure all changes have been entered, that the pages herein reflect the effective dates noted on changed pages, and that the plan is complete and accurate.

Revision No.	Date	Page(s)	Prepared By:	Approved

		Affected/Subject		By:
Initial	xxx	Initial issue of X plan	CSO	CEO
1	xxx	Appendix A and chapter 2.0-ship's details	CSO	CEO

INTRODUCTION-The ship security plan- Purpose

Commercial marine ships provide a target of opportunity for those desiring to commit criminal acts and inflict harm to others. This Ship Security Plan (SSP) has been developed to enhance the security of the ship and crew through awareness, prevention and response, thus reducing the risk of a security breach and associated consequences. This SSP was designed for ships involved in worldwide trading.

1.1 Objectives

To accomplish this Purpose, the Ship Security Plan will meet these objectives.

- Gather and assess information with respect to security threats, vulnerabilities and consequences, and incorporate appropriate mitigation measures;
- Provide and maintain communications protocols onboard and between ships and facilities;
- Prevent or deter unauthorized access to the ship and her restricted areas;
- Prevent or deter the introduction of prohibited weapons, incendiary devices, or explosives to ships;
- Provide a means for raising the alarm in reaction to security threats or security incidents;
- Develop and implement ship security procedures based upon the corresponding threat; and
- Train and drill to ensure familiarity with security plans and procedures.

This plan is written in accordance with and is intended to fully comply with:

- International Code of the Security of Ships and of Port Facilities - Part B, Annex to the International Convention of the Safety of Life at Sea, 1974 Chapter XI, as amended.

1.2 Company Security Policy

This Ship Security Plan contains polices and procedures to promote the security of the M.V. X.

During the development of the SSP, relevant provisions of the ISPS Code part B where taken into account by the company and has addressed those provisions of ISPS Code part B in the SSP, which are considered as relevant by the company.

Company shall comply with the relevant requirements of this chapter (SOLAS XI-2) and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

Ship shall comply with the relevant requirements of this chapter (SOLAS XI-2) and part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code, and such compliance shall be verified and certified as provided for in part A of the ISPS Code.

The Master has the overriding authority and responsibility to make decisions regarding the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

All crewmembers shall review the security instructions developed to implement this plan.

Maintaining ship security is an ongoing task. As potential new threats are uncovered, additional security measures and procedures might need to be implemented.

The Company shall ensure that the CSO and/or Alternate CSOs, Master and SSO are given necessary support to fulfill their duties and responsibilities in accordance with the security requirements set forth in the ISPS Code.

Only the Company Security Officer (CSO) and/or Alternate CSOs are authorized to release security information to the Master, Ship Security Officer (SSO), and Port Facility Security Officer (PFSO). Unless approved by the SSO, internal and external communications from the ship regarding security measures, threat analyses, intelligence information, and planned responses are not to be discussed with anyone on shore or to other members of the crew.

The Company Security Officer may delegate duties to be performed by the Ship Security Officer. Nevertheless the responsibilities rest always to CSO.

As required by the IMO, the company shall provide the Master of the ship at all times the name of the person or organization who appoints the members of the crew or other persons employed or engaged on board the ship in any capacity on the business of the ship is Y Shipping Co. Ltd. – Crewing Department.

Their address and contact information will be found in Appendix V.

All ship personnel are to:

- Assist the Ship Security Officer (SSO) and report security violations.
- Assist the SSO with the implementation of ship security bills and reporting discrepancies in those bills.

1.3 Approval of Ship Security Plan

The Ship Security Assessment was carried out according to the ISPS Code. The SSA report has been reviewed by the CSO and accepted by the company. The company retains a copy of the SSA report.

The Flag State or its Designated Authority within the government approved the Ship Security Plan. The original written verification of Plan approval(s) is handled in accordance with company policy and a copy is inserted in the Plan by the SSO.

1.4 International Ship Security Certificate

The Flag State also verified ship compliance with the provisions of SOLAS Chapter XI-1 and Part A of the International Ship Security Code, and issued an International Ship Security Certificate. The original certificate is kept on board in the Classification &Trading File and a copy of the certificate is maintained in Appendix B of this manual.

The International Ship Security Certificate is subject to port State control inspections but such inspections should not normally extend to examination of the Ship Security Plan itself. The ship may be subject to additional control measures if there is reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

1.5 Definitions

Calling Port: Port where a ship moors (or anchors) and crew are allowed to leave the ship to visit the port. Crew baggage and ship stores will not normally be loaded or off-loaded at calling ports.

Company: means the owner, organization, or person who is responsible for the operation of the ship.

Company Security Officer (CSO): The company official from the ship operator who will be responsible for developing, maintaining and enforcing the company security policies as set out in this document.

Declaration of Security (DoS): means an agreement reached between a ship and port facility or another ship specifying the security measures each will implement.

Disembark: Refers to any time that the crew leave the ship, be it a port call or final destination.

Embark: Refers to any time that crew board the ship, be it a port of call or initial boarding of the ship.

ISSC: means International Ship Security Certificate required by SOLAS and the International Ship and Port Facility Code.

MARSEC: means Maritime Security as used by the U.S. Coast Guard to designate security levels.

Operator: The person, company, or government agency, or the representative of a company or government agency, which maintains operational control over a terminal that the ship will visit.

Port: means the area, through which ship traffic and maritime commerce flow or people are transported, including areas ashore (extending to inter-modal and cargo storage areas) and on the adjacent water (to include anchorages and approaches), as defined by the designated authority.

Port Facility: is a location where the ship/port interface takes place, including anchorages, berths, and approaches.

Port Facility Security Officer (PFSO): a Person designated as responsible for the development, implementation, revision, and maintenance of the port facility security plan and for liaison with the port authorities and Ship Security Officers and Company Security Officers.

Recognized Security Organization (RSO): means an organization with appropriate expertise in security and anti-terrorism matters recognized by the Administration [or the designated authority] and authorized by it to carry out assessment, verification, approval and certification activities, required by SOLAS Chapter XI-2 or by Part A of the ISPS Code, on its behalf.

Security Incident: means any suspicious act or circumstance threatening the security of a ship.

Security Level: means an action level established by an Administration or Contracting Government that represents their assessment of the likelihood that a security incident will be attempted or will occur.

Ship: means any vessel, including mobile offshore drilling units, barges, small passenger vessels, etc., that is required to have an International Ship Security Certificate or other security certificate required by a government.

Ship/Port Interface: means the interactions that occur involving movement of people, goods or provisions of port services to or from the ship.

Ship Security Assessment (SSA): A risk based analysis of security-related hazards or threats for each ship the Company operates. The SSA should address the particulars of the ship, its cargoes and crew, and the locations where it will operate. It should also consider the likelihood of various security-related scenarios and possible responses to those scenarios.

Ship Security Officer (SSO): The specific individual onboard the ship who is designated by the Company. The SSO reports to the Master for the overall management and oversight of all shipboard security policies, programs and procedures. The SSO is identified by name and position on the ships crew list and in the advance notice of arrival.

Ship Security Plan (SSP): A ship specific document based on the SSA that identifies equipment, measures, and procedures that are to be employed to maintain security on board the ship. The plan must address specific measures appropriate to the level of security specified by the Government or Company.

Ship-to-Ship Activity: means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

Terminal: Any structure used for the assembly, processing, embarking, or disembarking of cargo for the ship. It includes piers, wharves, and similar structures to which a ship may be secured; land and water under or in immediate proximity to these structures; buildings on or contiguous to these structures; and equipment and materials on or in these structures.

Unlawful Act: An act that is a violation under the laws of the states where the ship is located, or under the laws of the country in which the ship is registered.

Voyage: The ship's entire course of travel, from the first port at which the ship loads cargo until its return to that port or another port where the majority of the cargo is offloaded and the ship terminates that voyage.

Security Levels:

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 transportation 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 transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

1.6 Acronyms and Abbreviations

CSO:	Company Security Officer
DOS:	Declaration of Security
ISPS Code:	International Ship and Port Facility Security Code
ISSC:	International Ship Security Certification
MARSEC:	Maritime Security
PFSO:	Port Facility Security Officer
RSO:	Recognized Security Organization
SSA:	Ship Security Assessment

SSO: Ship Security Officer

SSP: Ship Security Plan

SHIP DETAILS

1.7 General Information

Ship Name: ____

Flag: ____

IMO #: ____

Call Sign: ____

Official #: ____

Sat Comm. #: ____

Ship Owner: ____

Owner Address: ____

Operator: ____

Operator Address: ____

Operator’s Phone: ____

Operator’s Fax: ____

1.8 Ship Physical Characteristics

Port of Registry: ____

Shipyard: ____

Year Built: ____

Hull Type: ____

Class: ____

Overall Length: ____

Maximum Beam:

Depth:

GRT:

NRT:

Summer DWT:

2.0 HIP SECURITY ORGANIZATION

2.1 Ship Security Organization

The Company Security Officer, Ship Security Officer, Security Patrol and Security Team are designated as shown in this organization chart to perform the duties assigned in the Ship Security Plan. See in the text for CCEO.

2.2 Designation of Company Security Officers

The company designates the Company Security Officer (CSO) and the alternates CSOs .Their names have been issued and has been distributed to all shore-based operations management personnel and shipmasters and has been posted in the company office and on company ships**.**

Should the person designated as CSO and/or alternate CSO change, a subsequent announcement will be issued, distributed and posted as previously described.

Company Security Officer and alternate CSOs contact information will be found in Appendix I.

2.3 CSO Duties and Responsibilities

The Company Security Officer is assigned and will fulfill the following duties and responsibilities:

- Advice what threats may be encountered by the ship(s), using appropriate security assessments and other relevant information.
- Ensure ship security assessments and annual reassessments are carried out.
- Ensure the development, the submission for approval, and thereafter the implementation and maintenance of the Ship Security Plan.
- Ensure the Ship Security Plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship.
- Arrange for internal audits and reviews of security activities.
- Arrange for the initial and subsequent verifications of the ship by the Administration or Recognized Security Organization (RSO).
- Ensure that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections, and verifications of compliance are promptly

addressed and dealt with.

- Enhance security awareness and vigilance within the organization.
- Ensure adequate training for personnel responsible for the security of the ship.
- Ensure effective communication and cooperation between the Ship Security Officer (SSO) and the relevant Port Facility Security Officer (PFSO).
- Ensure consistency between security requirements and safety requirements.
- Ensure that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately.
- Ensure security measures give particular consideration to convenience, comfort, and personal privacy of ship personnel and their ability to maintain their effectiveness over long periods.
- Provide ship Master with information relating to parties responsible for, (a) appointing shipboard personnel, (b) deciding employment of the ship, and (c) charter party details (Appendix V); and,
- Ensure that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

The successful completion of these duties will be assessed annually through the company's normal personnel evaluation program by his direct supervisor.

Alternate CSO: The alternate CSOs are the delegates of the CSO. The alternate CSO takes over the CSO duties and responsibilities of the CSO when he is unavailable. The Alternates CSO take action in turn as described in Appendix I. Alternate CSOs are authorize to have direct access with the vessel for security matters as to send security bulletins, information and/or instructions within the scope of the SSP in order to assist the effective CSO monitoring and follow up.

2.4 Master Responsibilities

The Master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request assistance of the Company or any Contracting Government, as may be necessary.

The Master shall not be constrained by the Company, the charterers or any other person from taking or executing any decision that, in the professional judgment of the master, is necessary to maintain the safety and security of the ship.

Although this excludes denial of access by any officer authorized by Contracting Government, the Master shall confirm that such an officer is duly authorized by means of verifying his identification document, etc.

If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the Master shall give effects to those requirements necessary to maintain the safety of the ship. In such cases, the Master implements temporary security measures and shall forthwith inform Administration, Company, and, if appropriate, Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures shall, to the highest possible degree, be commensurate with the prevailing security level.

Even at Security Level 3 the Master will seek clarification or amendment of instructions issued by those responding to security incident or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

The Master can request the assistance of the Company or of any Contracting Government as may be necessary.

2.5 Designation of Ship Security Officer (SSO)

The Ship Security Officer (SSO) is designated by the company. An announcement which names the SSO has been issued and distributed to all shore-based operations management personnel and the ship's master, in substantially the same form which follows. This announcement is also posted in the company office and on the company ship, where such information is normally displayed. A sample designation letter can be found in Appendix N.

Should the person designated as SSO change, a subsequent announcement will be issued, distributed and posted as previously described.

Chief Officer is designated as the deputy of SSO.

2.6 SSO and Deputy SSO Duties and Responsibilities

(A) The Ship Security Officer (SSO) is assigned and will fulfil the following duties and responsibilities:

- Conduct regular security inspections of the ship at least once a month. Those inspections are to be recorded in the Ship Security Log Book.
- Maintain and supervise implementation of the Ship Security Plan, including any amendments to the plan;
- Coordinate the security aspects of the handling of cargo, bunkers, and ship stores with other shipboard personnel and with relevant port facility security officers;
- Review the SSP and the SSA and propose any modification (if any) to the Ship Security Plan periodically but at least on an annual basis. SSO after assessing the SSP implementation and if he has any proposal to make he should send a written review to CSO or his delegates.
- Reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections, and verifications of compliance and implementing any corrective actions;
- Enhance security awareness and vigilance on board ship;
- Ensure that adequate training has been provided to shipboard personnel, as appropriate;
- Ensure the reporting of all security incidents and breaches of Security
- The Ship Security Officer (Master) and his delegate (Chief Officer) have custody of master Keys with access to all the Fixed Locks on board the vessel.
- Ensure the coordination of the ship security plan with the Company Security Officer and the relevant Port Facility Security Officer;
- Ensure that security equipment onboard the ship is properly operated, tested, calibrated and maintained, if any;
- Conduct security survey of port utilizing the Port Security Survey Form in Appendix J.
- Ensure consistency between security requirements and the proper treatment of ship personnel affected by those requirements; and
- Review and complete a Declaration of Security agreement.
- Provide security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

- Ensure that the SSP is kept confidential and at a secure place (ref. 5.2) and that the crew is familiar with the contents of the plan as appropriate.

The successful completion of these duties will be assessed annually through the company's normal personnel evaluation program by his direct supervisor with input from the Company Security Officer. Without exception, the Master (if not the SSO) continues to have the overriding authority and responsibility to make decisions with respect to the security of the ship and to request assistance, as needed.

(B) “Deputy SSO” Duties and Responsibilities

Chief Officer is designated as deputy SSO. Deputy SSO takes over the duties of SSO, whenever the latter is not able to perform them, but the responsibilities remain always to SSO.

2.7 Liaison with Waterfront Port Facility Security Officer (PFSO)

The SSO will provide liaison on behalf of the ship to the PFSO representing the waterfront facility. The primary purpose of this liaison is to exchange critical security information and coordinate security arrangements between the ship and the facility. Topics to be discussed include the following:

- Any current threats. The current Marine Security level.
- Communications procedures to report a security incident or threat.
- Facility security arrangements. Ship security arrangements.
- Control of access to the facility and ship. Screening of personnel and baggage.
- Security requirements for cargo handling operations; and Declaration of Security, when required.

2.8 Security Patrols

All ship crewmembers have the responsibility to be vigilant and aware of possible security vulnerabilities and breaches. Should a crewmember observe a security breach, they are instructed to report it immediately to the Duty Officer, who will then notify the Ship Security Officer.

When enhanced security monitoring is required, the Master may implement Security Patrols. Those persons identified on the security organization chart (3.1) may be assigned to a Security Patrol. Additional persons may be assigned to perform Security Patrol duties as determined necessary by the Master. The duties of the

Security Patrol are as follows:

- Monitor assigned areas at a set frequency for security breaches.
- Report security breaches to the Duty Officer.
- Attempt to mitigate the impacts of a security breach, to the extent training and standard operating procedures permit, and,
- Ensure the access controls are in place and operating properly (e.g. doors locked, intruder alarms, set).

Security Patrols shall be trained in these duties and specific response procedures contained in this plan. Also, Security Patrols will be provided with a means of communications. Security Patrols will be required to check-in with the Duty Officer every 15 minutes.

2.9 Security Team

If a security incident occurs, a response by the ship crew may be necessary. Such a response will be carried out by a Security Team, which is made up of those persons designated on the security organization chart in Section 3.1. The Master may assign additional persons to the Security Team as determined necessary.

The designated Security Team Leader is the Ship Security Officer (Master) or his delegate.

The Security Team will implement whatever actions are necessary to secure the incident, protect the crew, ensure the safety of the ship and minimize impacts to the surrounding area.

Security Team members will be trained in their duties and equipped to perform these duties. All appropriate precautions will be taken to protect the Security Team during a response.

TRAINING, DRILLS, AND EXERCISES

2.10 Procedures for Training

The Company Security Officer, Ship Security Officer, and appropriate shore-based personnel generally will have knowledge and receive training taking in their areas of responsibility. Ship personnel having specific security duties will understand their responsibilities for ship security as described in the Ship Security Plan and generally have sufficient knowledge and ability to perform their assigned duties.

The Company Security Officer and appropriate shore-based personnel and the SSO shall have knowledge of and receive training in some or all of the following as appropriate:

- Security administration.
- Relevant international conventions, codes, and recommandations.
- Responsibilities and functions of other involved organizations.
- Relevant government legislation and regulations.
- Methodology of the ship security assessment.
- Security surveys and inspections.
- Ship and local port operations and conditions.
- Emergency preparedness and response and contingency planning.
- Instruction techniques for security training and education including security measures and procedures.
- Methods of handling of security related information and security related communications;
- Knowledge of current security threats and patterns.
- Recognition and detection of prohibited weapons, dangerous substances and devices.
- Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security.
- Techniques used to circumvent security measures.
- Security equipment and systems and their operational limitations.
- Inspection, control and monitoring techniques.
- Methods, policy, and procedures of physical searches.
- Security drills and exercises including drill with port facilities.
- Assessment of security drills and exercises.

In addition the SSO should have adequate knowledge of and receive training in some or all of the following as appropriate:

- Layout of the Ship.

- The ship security plan and related procedures.
- Operation of security equipment and systems.
- Testing, calibration and at-sea maintenance of security equipment and systems

Ship board personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

- Knowledge of current security threats and patterns.
- Recognition and detection of prohibited weapons, dangerous substances and devices.
- Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security.
- Techniques used to circumvent security measures.
- Crowd management and control techniques.
- Security related communications.
- Knowledge of emergency procedures and contingency plans.
- Operation of security equipment and systems.
- Testing, calibration and at-sea maintenance of security equipment and systems.
- Inspection, control and monitoring techniques.
- Methods of physical searches of persons, personnel effects, baggage, cargo, and ship stores.

These personnel shall include all officers and A/Bs. The SSO shall provide the above training.

All other ship board personnel shall have sufficient knowledge of relevant provisions of the SSP including:

- Meaning and the consequential requirements of the different security levels.
- Knowledge of emergency procedures and contingency plans.
- Recognition and detection of prohibited weapons, dangerous substances and devices.
- Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures;

The SSO shall provide the above familiarization to all other shipboard personnel when signing on.

Training that is provided will be documented, detailing the course date, content and attendees. The SSO will maintain this training information with other security sensitive information.

2.11 Procedures for Drills

Drills must test individual elements of the Ship Security Plan, including response to security threats and incidents. Drills should take into account the types of operations of the ship, ship personnel changes, and other relevant circumstances. Drills examples include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement.

Drills will be conducted at least once a quarter, unless the special circumstances of the ship type and ports to be visited suggest otherwise, i.e. at shorter or longer intervals, and if there are significant changes to the Ship Security Plan or the composition of the ship's personnel. An annual Security Drills Program is issued by the CSO and distributed to Company's ships.

Security familiarization for each signed on crewmember to be conducted by SSO or his deputy within the first 24 hours on board the first part and within 7 days the second part as described in the attached form. The form to be sent to Y upon completed.

Note: Drills must be conducted within one week whenever the percentage of ship personnel with no prior participation in a ship security drill on that ship exceeds 25 percent.

All drills will be documented, detailing the specific scenario, date, time, participants and areas for improvement. F110 (Record of drills for each seafarer to be completed).The SSO will maintain a log of all drills.

2.12 Procedures for Exercises

The objective of exercises is conduct a full test of the security program and must include the substantial and active participation of the CSO, PFSO, relevant authorities, as well as other SSO's if available. These exercises should be conducted with at least one of the Company's ships and should test communications, coordination, resource availability and response and may by:

- Full scale or live.
- Tabletop simulation or seminar.
- Combined with other appropriate exercises, or,
- A combination of the elements of the above three.

Each exercise must test communication and notification procedures, and elements of coordination, resources availability, and response.

Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises. All exercises will be documented, detailing the specific scenario, date, time, participants and areas for improvement. The SSO will maintain a log of all exercises.

A Drill and Exercise Schedule can be found in Appendix I.

3.0 RECORDS AND DOCUMENTATION

3.1 Records

In preparation to produce information to the control of Contracting Government, the following records within the period of the last 10 calls at a port facility, shall be retained at least 5 years.

§ Security level at which the ship operated in a port where it has conducted a ship/port interface;

§ Any special or additional security measures that were taken by the ship in a port where it has conducted a ship/port interface;

§ That the appropriate ship security procedures were maintained during any ship to ship (STS) activity, and,

§ Provisions of ISPS code B/4.37 and 4.38

Ø Measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government (especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments;

Ø Declarations of Security that were exchanged with port facility or other ship;

Ø Measures taken while engaged in a ship to ship activity with a ship flying the flag of a State which is not a Contracting Government especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;

Ø Measures taken while engaged in a ship to ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions of chapter XI-2 and part A of ISPS Code (such as a copy of any security certificate issued to that ship under other provisions); and,

Ø In the event that persons or goods rescued at sea are on board, all known information about such persons or goods (ID certificate or result of any checks).

The Ship Security Officer must keeps records of the following activities for at least 5 years as specified by the administration, and makes them available to duly authorized personnel of Contracting Governments upon request:

§ Training, drills and exercises; Security threats and security incidents;

§ Breaches of security; Changes in Security levels;

§ Communication relating to the direct security of the ship, such as specific threats to the ship or to port facilities the ship is in or has been in;

§ Internal audits and reviews of security activities; Periodic review of the Ship Security Assessment;

§ Periodic review of the Ship Security Plan; Implementation of amendments to the plan; and,

§ Maintenance, calibration and testing of any security equipment provided on board, including the testing of the Ship Security Alert System.

The records shall be kept in the working language of the ship and if not already the working language of English. The records may be maintained in an electronic format. The Master shall protect the records from unauthorized access or disclosure in a secure location onboard the ship such as Master's cabin/safe.

A Security Daily Occurrence Log is maintained by the SSO.

Upon completion, all Daily Occurrence Logs are to be retained onboard for one year, after which they are to be forwarded to the CSO. Copies of serious incidents noted in the log are to be transmitted to the CSO via e-mail or fax within 24 hours of the incident occurring.

3.2 Plan Security Control

The Ship Security Plan contains highly sensitive information and, therefore, will be treated as confidential. The distribution, disclosure and availability of information contained in the plan will be strictly controlled and protected from unauthorized access. If the officers of a contacting government have clear grounds that the ship is not in compliance with the ISPC, and the only means to verify is to review the relevant requirements of the SSP, limited access is allowed and always with Master's consent. Nevertheless the sections 10, 12, 16 & Appendix P are considered as confidential as per ISPC Part A/9.8.1 and cannot be subject to inspection unless otherwise agreed by the contracting governments concerned.

A printed copy of the Ship Security Plan and other security sensitive material will be maintained locked to a location in the Master's office. The goal is to prevent access to this sensitive information by possible internal or external perpetrators. However SSO has to make sure that all officers are aware of the SSP content. Officers should acknowledge that their awareness by signing the acknowledgement page in the front part of the subject manual with the SSO presence.

4.0 MARITIME SECURITY (MARSEC) LEVELS

4.1 Maritime Security (MARSEC) Levels

The Master or the SSO is responsible for declaring the Ship Security Level. Security Levels or readiness conditions are procedures to respond to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface. Normal operating conditions are Security Level 1. At this readiness condition, the following actions are required for all ships:

- Ensure the performance of all ship security duties.
- Monitor access to the ship.
- Monitor the deck areas and areas surrounding the ship.
- Monitor the embarkation of persons and their carry-on items.
- Supervise the handling of cargo and ship’s stores.
- Ensure that port-specific security communication is readily available.

As the threat alters, the security level should be modified. The highest security level, as a general policy, may include arming ship personnel. Three Security Levels, or Security Readiness Conditions (SRC), have been established to respond to potential threats:

Security Level 1 Low – Threat Normal operating conditions.

Security Level 2: Medium Threat – Heightened threat due to an announcement or intelligence of a non-specific (perceived) threat.

Security Level 3: High Threat – Highest threat level in response to an attack or official information of a specific threat. It is important that Security Levels be clearly defined for all personnel. Training should be conducted at all readiness conditions to ensure rapid response to changing threats.

When entering a port, a ship is required to act upon the security level set by the Contracting Government. When the level changes from the Flag administration the CSO and/or the alternate CSOs should inform the ship by forwarding the relevant instructions. SSO has to acknowledge receipt of such instructions.

A ship, Company or Administration may choose a higher security level than recommended by the Port Facility Security Officer.

The SSO is required to liaise at the earliest opportunity with the PFSO to coordinate and establish the appropriate Security Level as required by the Contracting Government. The PFSO should advise the ship of any subsequent change in security levels established by the Contracting Government.

At Security Levels 2 and 3, a ship is required to acknowledge receipt of the designated authority's advice on a change in the security level. The SSO shall confirm to the Port Facility Security Officer the Ship's Security Level and report any differences of implementation.

For U.S. Ports: The Ship Security Officer must insure that prior to entering a port all measures are taken that are specified in this plan for compliance with the MARSEC Level in effect for the port. The U.S. Coast Captain of the Port (COTP) must be notified when compliance with a higher MARSEC Level has been attained and such compliance must be in place within 12 hours of notification of the requirement for a higher MARSEC Level.

At all times the Master has the ultimate responsibility for the safety of the ship. If, in the judgment of the Master, a higher MARSEC level is warranted, he should issue orders to raise the level for all onboard operations. However, while the ship may be operating at a higher security level, there will be no circumstances when the ship will have a lower MARSEC level than is declared by the port. If the Master believes that compliance with security instructions issued by those responding to a security incident may imperil the safety of the ship, the Master should seek clarification or amendment of these instructions.

4.2 MARSEC Level 1

At this security level, the ship crew will carry out all normal security duties and implement routine security procedures contained in this plan. These board preventive and protective measures may include the following:

- Ensuring the performance of all ship security duties;
- Monitoring restricted areas to ensure that only authorized persons have access;
- Controlling access to the ship;
- Monitoring of deck areas and areas surrounding the ship;
- Controlling the embarkation of persons and their effects;

- Supervising the handling of cargo and ship's stores and bunkers; and
- Ensuring that port-specific security communication is readily available.

4.3 MARSEC Level 2

At this security level, the ship crew will enhance security prevention and protective measures by implementing specific duties and security procedures identified in this plan. In general, the area of awareness will be extended and surveillance measures will be increased by implementing the following preventive and protective measures:

- Briefing ship officers and crew with security responsibilities on the increased threat; Increasing the frequency of monitoring restricted areas;
- Establishing routine Security Patrols; Reducing the number of access points to the ship;
- Posting personnel to guard access points; Minimizing the number of personnel permitted to board the ship;
- Increase the frequency of inspection of baggage and ship stores; and,
- For U.S. Ports: Briefing of ship crew of identified threats, reporting procedures and the need for increased vigilance.

4.4 MARSEC Level 3

At this security level, the ship crew will implement the highest level of preventive and protective security measures identified in this plan. In addition to activities specified for Levels 1 and 2, the Master may implement the following general actions, as appropriate:

- Post personnel to continuously guard critical restricted areas, such as the bridge and engine room.
- Increase the frequency of or establish continuous Security Patrols.
- Place the Security Team on alert.
- Limit access to the ship to a single point, which is continuously guarded.
- Restrict access to the crew and governmental authorities or those responding to a security incident or threat in a MARSEC Level 3 situation.
- Request waterside board patrols.

- Inspect all baggage and ship stores, and,
- Coordinate enhanced security measures with the port and facility.

For U.S. Ports: At MARSEC Level 3 the ship may be required to implement additional measures as required by the U.S. Coast Guard that may include but not limited to:

- Arrangements to ensure that the ship can be towed or moved if deemed necessary.
- Use of waterborne security patrol.
- Use of armed security personnel to control access to the ship and to deter to the maximum extent practical a Transportation Security Incident (TSI), or,
- Screening the ship for the presence of dangerous substances and/or devices underwater or other threats.

Specific security duties and procedures will be implemented for each activity identified in this Plan. Response to a security incident will be in accordance with this Plan.

For U.S. Ports: If for any reason the ship cannot comply with any U.S. Port requirements the COTP must be informed and approval obtained prior to entering any port, interfacing with another ship or with a facility or to continuing operations.

4.5 General Requirements for Security

	Security Level		
Protective Measure	1	2	3
All ship crewmembers will review and exercise their security duties and responsibilities through drills and training.	YES*	YES*	YES*
Provide security information to all crewmembers and any security personnel that includes the security level and any specific threat information.	YES	YES	YES
SSO will communicate with the port and specific waterfront facility to coordinate protective measures.	YES	YES#	YES#

* Drills and exercises are conducted quarterly.

# Coordinate additional protective measures.

4.6 United States Homeland Security Advisory System (HSAS)

The below table shows the relationship between the United States HSAS and the Maritime Security Levels:

Homeland Security Advisory System (HSAS) Threat Condition	**Equivalent Maritime Security (MARSEC) Level**
Low: Green	MARSEC Level 1
Guarded: Blue	MARSEC Level 1
Elevated: Yellow	MARSEC Level 1
High: Orange	MARSEC Level 2
Severe: Red	MARSEC Level 3

HIP/WATERFRONT FACILITY INTERFACE

4.7 Procedures for Interfacing with Port Facilities

Prior to arrival at the waterfront facility or a location for ship-to-ship interface the Ship Security Officer or the Duty Officer acting as his delegate will contact the designated Facility Security Officer or Ship Security Officer representing the waterfront facility or ship. The purpose of this communications is to exchange critical security information and coordinate security arrangements between the ship and the facility. Topics to be addressed include:

§ Communications established between the ship(s) and/or waterfront facility;

- Means of raising alarm agreed between ship(s) and/or waterfront facility,
- Ship/waterfront facility report/communicate any noted security non-conformities and notify appropriate government agencies, and
- Port specific security information passed to ship and notification procedures established (specifically who contacts local authorities, National Response Centre and Coast Guard),

§ Responsibility for checking identification and screening of

- passengers, crew, hand-carried items, and luggage,
- ship stores, cargo, and vehicles

§ Responsibility for searching the berth/pier directly surrounding the ship.

§ Responsibility for monitoring and/or performing security of water surrounding the ship.

§ Verification of increased MARSEC level and implementation of additional protective measures, and,

§ Establish protocol to coordinate response between ship/waterfront facility to acts that threaten either the ship and/or waterfront facility.

4.8 Procedures for Interfacing with a Dry-docking

Prior to arrival at the dry docking facility, the CSO has to contact with the dry docking Security officer in order to exchange critical security information and coordinate security arrangements between the ship and the shipyard facility. Relevant instructions are to be given to SSO and any particular security measure to be taken is to be logged in the Security Log. SSO to conduct Security survey and to complete Declaration of Security as necessary. *(Ref. to YEN Circular/ 3725.1/106/05/04-07-2005 YEN/ΚΝΠ/ΔΕΔΑΠΛΕ Β΄ – Γ΄).*

DECLARATION OF SECURITY

4.9 Declaration of Security (DoS)

Ships may be required to complete a DOS depending on MARSEC levels and cargoes handled. In addition, the Contracting Government may require at any time, at any MARSEC level, that a Declaration of Security (DoS) be completed and signed by the ship and facility representatives to document agreement on security responsibilities listed above. A sample Declaration of Security is included in Appendix K.

The Declaration of Security may be completed by:

- The Ship Security Officer, or designated person on behalf of the ship; and;
- The designated representative on behalf of the waterfront facility.

A change in the security level may require that a new or revised DoS is completed. SSO is to take always into consideration the updated circulars issued by the flag state regarding the issue of Dos.

(Ref. to YEN Circular / 3725.1/123/05 / 19-07-2005 ΥΕΝ/ΚΝΠ/ΔΕΔΑΠΛΕ Β΄ - Γ΄)

Both the ship and the waterfront facility generally keep a copy of the Declaration of Security and a copy is to be sent to the CSO. However, the DoS do contain sensitive information and appropriate measures should be taken to ensure that its confidentiality is protected. The Declaration of Security may be made available to port state authorities or their representative upon request.

4.10 DoS Procedures

At Security Level 1, a DoS is completed and signed by the SSO with the PFSO, or their designated representative, of any ship or port facility with which it interfaces.

§ For a ship-to-facility interface, prior to arrival to a facility, the PFSO of the port facility and the SSO or their designated representatives coordinates security needs and procedures, and agree upon the contents of the DoS for the period of time the ship is at the port facility. Upon arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the PFSO of the facility or SSO, or designated representatives sign the written DoS.

§ For a ship-to-ship interface, prior to the interface, the respective SSO, or their designated representative coordinates security needs and procedures, and agree upon the contents of the DoS for the period of time the ships are interfaced. Upon the ship-to-ship interface and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective SSOs, or designated representatives sign the written DoS.

At Security Levels 2 and 3, SSO, or designated representative sign and implement a DoS prior to any ship-to-ship interface.

At Security Levels 2 and 3, SSO, or designated representative of any ship sign and implement a DoS with the PFSO of any port facility on which it calls prior to any cargo transfer operation or passenger embarkation or disembarkation.

At Security Levels 1 and 2, the SSO implements a continuing DoS for multiple visits with port facilities that are frequently interfaced provided that:

§ The DoS is valid for the specific Security Level;

§ The effective period at Security Level 1 does not exceed 90 days; and

§ The effective period at Security Level 2 does not exceed 30 days.

When the Security Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS is signed and implemented in accordance with this section.

The port authorities may require at any time, at any Security Level, to implement DoS with the SSO or PFSO prior to any ship-to-ship or ship-to-facility interface when he or she deems it necessary.

COMMUNICATION AND COORDINATION

4.11 Ship

The Ship Security Officer will utilize the on board alarm system to alert ship personnel of changes in security conditions on board the ship.

A suitably qualified General Operator should be on duty at all times when ships are in, or approaching areas where attacks occur or may occur. One of the qualified G/O other than the Master shall be called upon to be the Designated General Operator. In addition to the Navigating Officer, it is advisable to have a duly qualified dedicated G/O to perform the GMDSS Watch, to ensure the ship's bridge is adequately manned when transiting potentially hazardous waters.

Prior to entering areas where attacks have occurred or where intelligence indicates attacks may occur, General Operators should practice and perfect pertinent radio operational procedures and ensure all transmitters, including satellite earth stations are fully operational and available for immediate use on distress and security frequencies. Where an INMARSAT ship earth station is provided it is appropriate to draft and store "standard messages" for ready use in an emergency. Masters should ensure that all procedures to generate a distress alert on any communication equipment are clearly marked on, or near, the equipment and all appropriate crewmembers briefed on their operation.

A special Code for piracy/armed robbery/attack is available for use on digital selective calling (DSC) equipment. DSC equipment shall be modified to incorporate this facility. The Company is responsible for making sure the Company Security

Officer and the Ship Security Officer have communicated with Coast State and Port Authorities to develop the list of contacts needed to establish a plan that works.

The Master and all Radio Operators should be aware that potential attackers might be monitoring ship to shore communications and using intercepted information to select targets. When transmitting information regarding cargo, valuables and the status of ship’s stores, caution is advised.

The master or senior officer available shall make sure that the appropriate Contracting Government authorities are contacted to report any suspicious movements, which may result in imminent attack, and Piracy, Armed Robbery or Terrorist attacks.

In addition, if the Master believes the other ship’s movement constitutes a direct threat to his ship or a danger to navigation in general, he shall consider sending an “All Stations (CQ) “danger message” as well as advising the appropriate Contracting Government authority. A danger message should be transmitted in plain language on a VHF working frequency following an announcement on VHF Channel 16 and or transmission of a DSC Call on VHF Channel 70 using the “safety” priority. All such messages shall be preceded by the safety signal (SECURITE).

When the Master has concluded that the safety of the ship is threatened, he shall:

§ Activate the Security Alert, and,

§ Notify the cognizant Contracting Government authority and if considered appropriate authorize a broadcast of an “All Stations” “Urgency Message” on VHF Channel 16, 2182 kHz or any other radio communications he considers appropriate (e.g. INMARSAT). Such messages shall be preceded by the appropriate Urgency Signal (PAN PAN) and or a DSC call on VHF Channel 70 and /or 2187.5 kHz.

When an attack has occurred and in the opinion the crew and ship are in grave danger requiring immediate assistance, the Master shall authorize the broadcast of a “Distress” message be preceded by the appropriate Distress alerts (Mayday, SOS, DSC, etc..) using the radio equipment most appropriate for the area taking into account the GMDSS Designation. The appropriate Contracting Government authority shall acknowledge receipt of the message and attempt to establish communications.

Masters shall bear in mind that the distress signal is provided for use in cases of imminent danger and it shall not be used for less urgent purposes.

4.12 Measures for Ensuring Port Specific Security Communication

	Security Level		
Protective Measure	1	2	3
Perform regular communications checks	YES	YES	YES
Provide a backup means of communication	YES	YES	YES#
# Provide a redundant and multiple means of communication			

4.13 Port

Prior to entering into a port or as soon as possible after arrival, the Ship Security Officer or the Duty Officer acting as his alternate will contact the designated port authority for security matters to obtain the latest security status and coordinate any special requirements.

Topics to be addressed include:

§ Current Maritime Security level; Any current threats;

§ Communications procedures to report a security incident or threat; and

§ Any special security requirement.

The information obtained from the port authority will be provided to the ship Master and recorded in the logbook, as appropriate.

4.14 Waterfront Facility

Prior to arrival at the waterfront facility or as soon as possible after arrival, the Ship Security Officer or the Duty Officer acting as his alternate will contact the designated Facility Security Officer representing the waterfront facility. The purpose of this communication is to exchange critical security information and coordinate security arrangements between the ship and the facility.

Topics to be addressed include:

- Any current threats; The current Marine Security level;
- Communication procedures to report a security incident or threat;
- Facility security arrangements; Ship security arrangements;

- Control of access to the facility and ship; Screening of personnel and baggage;
- Radio channel to relay information between parties and communications test;
- Security requirements for cargo handling operations; and,
- Declaration of Security, when required.

4.15 Law Enforcement

Security incidents and threats will be reported in accordance with the port and facility requirements. In most cases, the port or facility representatives will report these incidents and threats to law enforcement authorities. If required, the Master or Ship Security Officer will report appropriate security incidents and threats to law enforcement directly. In the event that emergency assistance is needed from law enforcement authorities, a request will be placed by the most expeditious method.

In all cases, the Master and ship crew will cooperate fully with law enforcement authorities regarding all security matters. The Ship Security Officer will be the primary point of contact for law enforcement representatives.

4.16 Company

The Company Security Officer (CSO) and/or the alternate CSOs and Ship Security Officer (SSO) will routinely communicate in order to coordinate related security duties. The communication may be established by phone or email or fax at the convenience of both parties.

The Company is responsible for making sure the Company Security Officer and the Ship Security Officer have communicated with Coast State and Port Authorities to develop the list of contacts needed to establish a plan that works.

SHIP SECURITY SYSTEMS AND EQUIPMENT MAINTENANCE

4.17 Security Systems and Equipment Maintenance

If the ship is equipped with security systems and equipment, that equipment must be in good working order and inspected, tested, calibrated, and maintained according to the manufacturer's recommendation. The CSO should ensure that the recommended service is carried out properly.

The results of such testing shall be recorded in accordance with the record-keeping requirements and F075 to be completed appropriately. Any deficiencies shall be promptly corrected.

If any equipment is inoperative or otherwise impaired while the ship is operating, the SSO shall report that fact to the CSO as soon as practicable and the latter is responsible to take the appropriate actions by all the available means to restore the problem.

The SSO is responsible for visually inspecting and/or testing any security equipment with which the ship is equipped, including, but not limited to, the following:

§ Audible or visual alarm systems; Communication systems;

§ Lighting controls; Locking and/or securing equipment.

Any deficiencies identified during security equipment inspections must be corrected immediately, if possible. If the needed corrective action cannot be performed by the SSO, the deficiency must be reported to the CSO. The CSO will then ensure that the necessary repairs are conducted by the appropriate maintenance personnel and document the action taken in accordance with the requirements.

4.18 Ship Security Alert System

Ship Security Alert System is installed to the ship. The Security Alert System, when activated, will send an emergency signal to the CSO and his delegates and to the Company's subcontractors OOPS (O'Briens – Contact Person: Calvin Kline). This signal will identify the ship and position, and will indicate that the security of the ship is under threat or has been compromised.

When the CSO and the designated authority (OOPS) are alerted, they have first to contact with the vessel to verify that the vessel is under threat. If the security alert system is activated by error then the CSO or the alternates are to reset it following the appropriate procedure.

If the security alert is confirmed and a real threat is identified on board then the CSO or the alternates CSOs or the designated authority OOPS (under CSO authorization) have to notify the Ministry of mercantile marine Joint Rescue Coordination Center, Piraeus (JRCCP) as described in Appendix P and the Contracting Governments in the vicinity of where the ship is operating.

The emergency alert system is designed so that the alarm will not be heard on board the ship or by other ships and will continue until the alarm is deactivated or reset. In other words the alarm is covert and will not alert the persons attacking the ship or another station linked with the attack. Activation points include the bridge and one other location designed below to avoid accidental initiation.

4.19 Location of Activation Point (other than Bridge)-Master's quarters.

4.20 Procedure to Start Activation

The SSO and his deputy shall start activation of the ship security alert system only when he judged that the security of the ship was under threat or it has been compromised. Nevertheless all officers shall be aware of the activation procedure but they shall proceed only when SSO and deputy are unable to do so.

At start of activation, pay attention on possible reaction of receiver of the alert, and give enough consideration on the prospective consequence caused by alert.

4.21 Method to Stop Activation

CSO or his alternates are the designed persons to reset the security alert. Procedure is described in Appendix P.

4.22 Method to Reset-As per Appendix P.

4.23 Inspection, Testing and Maintenance-Inspection/Maintenance: As per Appendix O.

Testing: The Ship Security Alert System is to be tested when initially installed on board, every 3 months and during every Safety Radio & GMDSS annual survey as per the manufacturer instructions. Records of the tests to be maintained by SSO and CSO.

4.24 Fire/General Alarms

Alarms such as the fire or general alarm may be of some use, particularly during an attack by pirates, where they may assist in frightening off the perpetrators. However in other cases, such as hijacking by terrorists, the sounding of such an alarm may cause the hijackers to panic and/or take violent action against the crew. Therefore, caution and due consideration is to be exercised before the sounding of an audible alarm.

4.25 Verbal Alarms

A covert word or phrase is to be used in order that crewmembers can pass word of an attack amongst each other. It is essential that the SSO ensure that all personnel are familiar with the word/code and what to do on hearing it. The word or phrase must not be written down.

ACCESS CONTROL-Access Control Procedures

Access points to the vessel include gangways, pilot ladders and mooring lines. The gangway is the only authorized access point to the ship while at port. The Pilot Ladder shall only be used when the gangway cannot be lowered. At such times this access point will be manned. Mooring lines are not considered authorized access points. Additional access points may be present depending on the port and facility.

The Company Security Officer has established the following procedures to describe what the Ship Security Officer shall do:

MARSEC Level 1: Verify everyone’s identity before allowed onboard.

§ Inspect persons and their belongings before being allowed onboard.

§ Limit and/or restrict access to critical Ship areas to authorized personnel.

§ The Main Gangway will be manned. Pilot’s Ladder is secured if not in use.

MARSEC Level 2: Assign additional personnel to guard access points.

§ Limit the numbers of access points to the Ship; identify closed access area and the means to secure them.

§ In coordination with a port facility, extend perimeter security beyond the immediate port area.

§ Increase the frequency of inspections of people, carry on items to deter and detect the introduction of weapons, explosives, etc.

§ The Main Gangway will be manned. Pilot’s Ladder is secured if not in use.

§ Security patrols to make periodic checks of mooring lines.

MARSEC Level 3

§ Assign additional personnel to guard access points and areas adjacent to access points.

§ Limit entry to the ship to a single access point. Protect electronic information systems.

§ The Main Gangway will be manned. Pilot’s Ladder is secured if not in use.

§ Security patrols to make periodic checks of mooring lines.

Access to the ship shall not be prevented for:

- Emergency or humanitarian reasons
- Security purposes (e.g. authorities in case of a bomb threat),
- If control measures according XI-2 / 9.1.3 or steps according XI-2 / 9.2.5 have been initiated by officers duly authorized?

4.26 Measures for Controlling Access to Ship

The following protective measures should be applied at the appropriate access locations at each security level, the types of restrictions to be applied, the means of enforcing them, and the frequency (random or occasional basis) of the application of these measures; all to be set by the company.

	Security Level		
Protective Measure	1	2	3
Access points are secured@ or continuously attended to prevent unauthorized access.	YES	YES#	YES#
Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access[1]	YES	YES	YES
Weather-deck access vents, storage lockers, and doors to normally unmanned spaces (such as storerooms, auxiliary machinery rooms, etc.) are locked@ or precautions taken to prevent unauthorized access.	YES	YES	YES
Limit entry to the ship to a minimum number of access points. +	NO	YES	YES*
Establishing a restricted area on the shore side of the ship, in close cooperation with the port facility.	NO	YES	YES

Carrying our a full or partial search of the ship	NO	YES	YES **
Conduct a stowaway search prior sailing	YES	YES	YES
Moving the ship	NO	NO	YES
Evacuating the ship	NO	NO	YES
Initiating measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.	NO	NO	YES

* Limit entry to a single access point when possible.

@ Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.

+ While not restricting egress from the ship in the event of an emergency.

# Assign additional personnel at appropriate access points as designated in the security plan.

** Preparing for a full or partial search of the ship and searching restricted areas as part of the search

RESTRICTED AREAS

4.27 Establishment of Restricted Areas

Restricted areas are spaces that are essential to the operation, control, or safety of the ship for which access must be limited to authorized personnel only. The Company Security Officer (CSO) has designated the following restricted areas.

1. Navigation Bridge and Radio Spaces Engine Room/Engine Control Room
2. Steering Gear Space. Emergency Generator/Battery spaces
3. Emergency Fire Pump Space. Fire Fighting Medium Storage Space
4. Fire Fighting Medium Release and Quick Closing Valve Activation Points
5. Cargo and Ballast Control Stations. Ventilation & Air Conditioning Equipment Spaces.
6. Oxygen/Acetylene Storage Spaces. Dangerous Chemical Storage Spaces
7. Cargo pumproom/ cargo instrumentation spaces. Lifeboat Launching Areas

8. Telephone Exchange. Stores and provisions and crew’s accommodation.

9. The Master my designate additional spaces as restricted areas, as deemed necessary.

The above areas are designated as restricted only during vessel’s stay in port and at anchorage. It applies to SSO discretion to reactivate the above areas during vessel’s voyage due to exceptional circumstances. Such activation/deactivation of restricted areas is to be entered in the Security Log Book.

4.28 Methods to Monitor and/or Restrict Access

All restricted areas are appropriately marked in such a way that these markings are visible to and the meaning known by the ship crew.

Monitoring and controlling access to restricted areas will normally be accomplished by the following means:

§ Doors and cabinets will be locked or secured at all times;

§ Crewmembers will ensure that doors and cabinets for restricted areas remain locked or secured; and,

§ Unsecured doors[6] and cabinets for restricted areas are reported to the Watch Stander.

In the event that the MARSEC level is increased to level 2, the Master may elect to implement the following additional security measures:

§ Initiate roving Security Patrols for specific areas and at set frequencies;

§ Posting personnel as guards at the entrance to critical restricted areas; and

§ Providing radios to Security patrols and guards, and requesting them to check-in with the Watch Stander at periodic intervals.

At MARSEC level 3, the Master may elect to implement the following additional security measures:

§ Increase the frequency of Security Patrols or establish continuous patrols;

§ Post guards at all entrances to restricted areas; and

Search all restricted areas on a periodic basis for security breaches.

[6] Doors in escape routes, which are locked or secured to restrict access, must be capable of being operated without keys from the direction for which escape is required.

4.29 Security Requirements for Monitoring Restricted Areas

Use following protect measures to ensure that only "Authorized Personnel" have access to the ship. Nevertheless SSO must ensure that restricted areas involved in ship's safety are always accessible to the ship's crew and in readiness in case of emergency.

	Security Level		
Protective Measure	1	2	3
Locking or securing access to restricted areas(areas involved in safety are to be secured with weak links only in order to be accessible by crew at all times)	YES	YES*	YES*
Using personnel as security guards or patrols	YES	YES**	YES***
Restricting access to areas adjacent to access points	NO	YES*****	YES*****

*. Increasing the frequency and intensity of monitoring and access controls on existing restricted areas

**. Dedicating additional personnel to guarding or patrolling restricted areas

***. Posting personnel to continuously guard restricted areas and/or assigning personnel to continuously

Patrol restricted areas and areas adjacent to restricted areas.

****. Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.

*****. Restricting access to additional areas

4.30 Intrusion Detection Devices

A monitoring camera is installed outside the internal bridge door in order the OOW to monitor the Bridge's entrance and allow access only to authorized personnel.

HANDLING OF CARGO, BUNKERS, AND SHIP STORES

4.31 Screening Procedures

Under normal conditions (MARSEC level 1), the following procedures will be used to supervise and secure cargo handling, bunkering, and loading of ship stores:

§ Verify that cargo loaded as per cargo manifest

§ Maintain a record of any dangerous goods or hazardous substances carried onboard, including an inventory and their location by utilizing the form in Appendix D;

§ Randomly inspect approximately 5-20% of the ship stores and provisions;

§ Ensure that ship's stores received to be loaded match ship's stores that were ordered.

Verification and inspection of cargo, bunkering, and ship's stores will be accomplished by:

§ Visage examination to identify evidence of tampering.

§ Coordinating with the shipper or other responsible party through an established agreement and procedures.

At MARSEC levels 2 or 3, the Master may elect to implement these additional security measures:

§ Suspension of cargo handling operations, bunkering, and the loading of ship's stores in cases of the most severe threats.

Increase the frequency of the inspection.

Measures for Supervising the Handling of Cargo, Bunkers and Ship’s Stores

	Security Level		
Protective Measure	1	2	3
Use of scanning/detection equipment, mechanical devices, or canines to check cargo.	N/A	N/A	N/A
Cargo Tank Domes inspected for tampering	YES	YES	YES
Coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures	YES	YES**	YES* *

Inspect ship's stores and provisions	YES**	YES*	ALL
In liaison with the facility, check seals or other methods used to prevent tampering	N/A	N/A	N/A
Restricting or suspending cargo and ship store operations	NO	NO	YES
Inspect ship stores prior to being brought on board	NO	YES	YES
Refusing to accept ship stores on board	NO	NO	YES
Being prepared to cooperate with responders and facilities	YES	YES	YES
Verify the inventory and location of any hazardous materials carried on board	YES	YES	YES
Ensure that the vessel fresh water intake is locked and secured	YES	YES	YES
* Increasing the frequency and detail of checking cargo, ship stores, and cargo spaces. This will ensure that only the intended cargo, container, or other cargo transport units are loaded **Increase the frequency, detail, and/or enhance			

MONITORING

4.32 Methods

Under normal operating conditions (MARSEC level 1), monitoring of deck areas and areas surrounding the ship will be assigned to all crewmembers in the course of their routine duties. The ship will rely on the waterfront facility for monitoring docks and the port for monitoring waterside areas.

At MARSEC level 2, the Master may elect to establish Security Lookouts or initiate Security Patrols. Lookouts will be positioned for maximum visibility of all deck areas, shore side facilities and waterside areas. Lookouts may move between two or three nearby locations to see all areas.

At MARSEC level 3, the Master may elect to implement the following additional security measures, while cooperating with those responding and the port facility:

§ Increase the number and frequency of security lookouts or Security Patrols to ensure continuous monitoring; Request waterside boat patrols at frequent intervals; and arrange for divers to inspect the underwater pier structures and hull, as deemed necessary.

4.33 Security Patrol Procedures

When Security Patrols are initiated, the following procedure will be observed:

§ Security Patrols will fulfil the duties specified in this Plan;

§ Security Patrols will be briefed at the start of their duty on the information known regarding potential threats;

§ Security Patrols will be provided with radios and portable lights, at a minimum;

§ Security Patrols will be assigned a specific area to patrol, depending on the potential threat, circumstances and available personnel;

§ Security Patrols will be instructed to report in to the Watch Stander or Duty Officer at 15 minute intervals;

§ Failure of a Security Patrol to report in as specified will result in attempts to contact the missing Security Patrol;

§ Failure to contact the missing Security Patrol will result in a search to locate the missing Security Patrol;

§ Failure to locate the missing Security Patrol after a ship-wide search will result in the notification of the Facility Security Officer, port and/or local law enforcement;

§ The Security Patrol will report all security incidents, suspicious events, unsecured restricted areas and alarming security devices to the Watch Stander or Duty Officer; and,

§ The Security Patrol will attempt to mitigate the impacts of a security breach, to the extent training and standard operating procedures permit.

4.34 Surveillance

Surveillance will be accomplished through crewmembers as a part of their normal assigned duties. At increased levels of security, Lookouts and Security Patrols may be utilized as previously described in the Plan.

4.35 Communications Procedures-Additional communication procedures can be found in Section 9.

In addition, it has been previously stated that Security Patrols and the Security Team will be provided with radios at the time they are activated. Radios will be utilized to routinely check-in, report security incidents and report the status of mitigation efforts to the Watch Stander and receive direction from the Master or Ship Security Officer.

4.36 Security Lighting

The ship will provide illumination of the deck and access points to the ship while conducting ship/waterfront facility interface activities. The ship will coordinate lighting with other entities involved in the ship/waterfront facility interface. While underway, the ship may consider using the maximum lighting available consistent with safe navigation in areas of a potential threat. The ship will consider the following in establishing the appropriate level and location of lighting:

§ Crewmembers are generally able to see beyond the ship, both pier side and waterside; Coverage normally includes the area on and around the ship; and

§ Coverage of access points and cargo handling areas.

At heightened MARSEC levels, additional lighting may be coordinated with the waterfront facility to provide additional shore side lighting. Additional lighting may include:

§ Turning on all available lighting; Using spotlights and floodlights to enhance visibility of the deck and areas surrounding the ship; and, using portable lighting to enhance visibility of the surrounding water and waterline. The emergency generator will operate critical security lighting and such lighting is designed to be operated in all weather conditions.

Measures for Monitoring Deck and Areas Surrounding the Ship.

	Security Level		
Protective Measure	1	2	3
Use security lookouts and/or security patrols	NO	YES**	YES**
Light deck and ship access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the ship*	YES	YES***	YES*****
In port – Light is provided to allow crewmembers to see beyond the ship, both pier side and waterside; including areas on and around the ship	YES	YES***	YES*****
Underway - maximum lighting available consistent with safe navigation and international regulation	YES	YES***	YES*****
In liaison with the port facility, perform waterside boat patrols to deter waterside access to ship and foot patrols or vehicle patrols on the shore side	NO	YES	YES****
Use divers to inspect the underwater pier structures prior to the ship’s arrival, upon the ship’s arrival, and in other cases deemed necessary and prepare for underwater inspection of the hull	NO	NO	YES****

* Coverage may be provided in coordination with a facility

** Increase the number and frequency of:

Security patrols during periods of reduced ship operations to ensure continuous monitoring; and

Waterside boat patrols to ensure continuous monitoring.

*At these higher security levels, additional lighting will be coordinated with the waterfront facility to provide additional shore side lighting. Additional lighting may include:

Using spotlights and floodlights to enhance visibility of the deck and areas surrounding the ship; and

Using lighting to enhance visibility of the surrounding water and waterline.

**** If required by port facility or if in response to specific threat information.

***** Switching on all lights, illuminating the vicinity of the ship

CONTROLLING EMBARKATION OF PERSONS AND PROPERTY

4.37 Identification and Visitor Control System

Control of embarking personnel and their personal property will be accomplished through the following identification, verification and control process:

§ All persons will be required to sign a register as they embark and disembark the ship in the Visitor’s Log Book (attached is F154)

§ All persons will be issued a security badge to be worn at all times while aboard and returned at the time of disembarkation;

§ The reason personnel are requesting to board the ship will be verified using tickets, boarding passes, work orders, delivery documents, or other means;

§ The identity of the person requesting to board the ship will be verified by use of a government issued photo identification, such as a passport, driver's license, identification card, government ID, or other similar means;

§ Arriving crew are verified as authorized to serve aboard the ship; and

§ A security briefing will be given to all passengers and newly boarded crewmembers on any specific threats, security awareness, compliance with all security measures in effect and reporting procedures for suspicious persons, objects and activities.

Note: Access may be denied to any person refusing to submit to security verification at a point of access. Each person denied entry for refusing may be identified and reported to appropriate authorities.

At MARSEC levels 2 or 3, the Master may elect to limit persons boarding the ship to essential personnel and government agents. Service providers and other persons needed aboard to provide essential services may be escorted while onboard. In cases of the most severe threats, the Master may suspend all access to ship and possibly order an evacuation of its crew.

4.38 Screening Procedures

It is the policy of this company that weapons, incendiaries, and explosives are banned from the ship as a condition of boarding. Under normal conditions (MARSEC level 1), the following procedures will be used to prohibit and prevent weapons, incendiaries and explosives from being brought onboard:

“Means of access” points include, but not limited, to:

§ Access ladders; Access gangways; Access doors, side scuttles, windows, and ports; Mooring lines and anchor chains; and Cranes and hoisting gear.

The following signs will be posted at appropriate access points;

- "Notice: All weapons are prohibited aboard this ship."
- "Notice: Boarding this ship is deemed valid consent to inspect vehicles, persons, articles and effects. Refusal of inspection will result in denied boarding and report to authorities."

§ Unaccompanied baggage will not be allowed on board.

§ Randomly inspect[7] approximately 5-20% of persons, baggage, carry-on items and personal gear for prohibited weapons, incendiaries and explosives;

[7] The purpose of the inspection is for private entities to secure their personal safety and safety of their property. Such inspections are intended to ensure that incendiary devices, explosives, or other items that pose a real danger of violence or a threat to security are not present. Inspections may be limited and no more intrusive than necessary to protect against the danger of sabotage or similar acts of destruction or violence. The inspection may, however, be reasonably effective to discover incendiary devices, weapons, explosives, and other implements of destruction. Inspection techniques may include, but are not limited to, magnetometers, physically examining the person or objects visually or through the use of trained animals, electronic devices, or combination of methods.

§ Persons found with weapons, other than duly authorized government agents, in their possession will be refused permission to board, or the Master may confiscate the weapon and place it in a secure area under lock during the voyage and return it upon disembarkation;

§ Designate persons to inspect baggage, carry-on items, and personal gear; and

§ Access to and from these areas will be controlled to segregate inspected persons and articles from un-inspected persons and articles.

At MARSEC levels 2 or 3, the Master may elect to implement the following additional security measures:

§ Increase the level of random inspections from 25% to 100%, depending on the nature of he threat;

§ Assign personnel to guard designated inspection areas.

Note: Access may be denied to any person refusing to submit to inspection at a point of access. Each person denied entry for refusing might be identified and reported to appropriate authorities.

4.39 Measures for Controlling the Embarkation of Persons and Effects

	Security Level		
Protective Measure	1	2	3
Verify reason personnel are embarking the ship by using joining instructions, tickets, boarding passes, work orders, pilot orders, surveyors orders, visitor badges, government identification, or other means.	YES	YES	YES
Suspending embarkation and disembarkation	NO	NO	YES
Positively identify crewmembers, vendors, visitors, and other personnel prior to each embarkation.	YES	YES	YES
Denying access to visitors who do not have a verified destination	NO	YES	YES
Verify arriving crew as authorized to serve aboard the ship.	YES	YES	YES
Inspect persons, baggage, carry-on items, and personal gear for *prohibited weapons*, incendiaries, and explosives.	YES**	YES	ALL
Security briefings provided to all persons on board, prior to departing, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.	NO	YES	YES*
Assign personnel to guard designated *inspection* areas.	NO	YES	YES
Limit entry to only crewmembers and other authorized personnel.	NO	YES	YES****
Escort all service providers or other personnel needed aboard to provide essential services to the ship.	NO***	YES***	YES***

* Security briefings are generally provided to all crewmembers, prior to each embarkation and disembarking.

** This may be accomplished by random *inspection*s, such as 5-20% or some other method addressed in the ship security plan.

*** All personnel allowed onboard are identified and approved at all security levels.

****Access is granted only to those responding to the security incident or threat there of and being prepared to cooperate with the responders and facilities.

4.40 Measures for Handling Unaccompanied Baggage

	Security Level		
Protective Measures	1	2	3
Ensure the checking of all unaccompanied baggage	YES	YES	YES
X-ray screening of all unaccompanied baggage provided that the equipment is available from the shore.	NO	YES	YES
Preparing restrict or suspend handling of unaccompanied baggage	NO	NO	YES
Refuse to accept unaccompanied baggage on board	NO	NO	YES

SECURITY INCIDENT PROCEDURES

4.41 Reporting Security Incidents

In the event of a security threat, security breach, or security incident, the person discovering the event will immediately report his observations to the Duty Officer or Watch Stander. The Duty Officer or Watch Stander will then immediately advise the Master and Ship Security Officer. The Master will determine what actions are necessary to ensure the safety of the crew and ship and protect the environment. The Master may order these actions to be taken by crewmembers or by the Security Team. If the Security Team is activated, the Ship Security Officer will act as the Team Leader, unless an alternate is designated.

The Security Team Leader will notify the Security Team to muster at a designated location. When the Security Team is present, they will be briefed on the nature of the security incident and the actions to be taken. All appropriate precautions will be taken to protect the Security Team during the response.

In the event that emergency assistance is needed from local law enforcement, this request will be made by the Master or his designee to the facility or port, ship's agent, or directly to the local law enforcement agency, whichever is faster. In any event, the facility and port will be advised of all significant security incidents. The CSO shall be contacted for contact details for (Point of Contact) if the ship needs to report a security concern about other ships, movements or communications or request advice or assistance from the (Point of Contact).

Reports of security incidents and suspicious activity will be entered into the ship's log. In addition, the Ship Security Officer should conduct an investigation of all security breaches. A report detailing the security breach, results of the investigation and corrective action recommended or taken should be prepared by the SSO and submitted to the Master and Company Security Officer.

SECURITY THREAT: A declaration to impose harm with the intent to cause a security breach or incident.

SECURITY BREACH: An incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded or violated.

SECURITY INCIDENT: An incident resulting in loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

4.42 Security Actions

Depending on the specific circumstances of a potential threat or security incident, the Master may elect to take any of the following actions:

- Securing all access to the ship to prevent intrusion;
- Performing emergency shutdown of main engine(s) to prevent unauthorized operation;
- Securing non-critical operations to focus attention on response;
- Alerting ship and shore-side authorities of an incident;
- Rendering assistance to a nearby ship undergoing an unlawful act;
- Responding to the detection of stowaways or intruders; Repelling boarders;
- Addressing a malfunction of onboard security equipment;
- Screening the underwater hull or search the ship in response to bomb threats;
- Specifying the kind of communications to use in the event of a breach of security, and unlawful act, or other emergency; and, Coordinating with waterfront facility response procedures.

When interfacing with an unsecured port or ship not covered by the International Ship Security Code or similar regulations, the crew will be on heightened alert. The Master shall implement interim security measures, such as those identified for MARSEC level 2 in this Plan.

The Master or SSO is responsible for filling out and submitting Security Incident Report, Appendix F, to the CSO within 24 hours of the discovery of any unlawful act. These reports should be kept on file with all other sensitive security information and copies provided to the Administration.

AUDITS AND SHIP SECURITY PLAN AMENDMENTS

4.43 Audits

The Ship Security Plan to be reviewed at intervals by the Company Security Officer to ensure its continued effectiveness:

- After lessons learned from: Audits, Drills, Exercises, and Security Incidents.

In addition, the SSP must be audited by CSO or his delegates if the following occurs: Change in company's operator; and/or modifications to ship including but not limited to physical structure, emergency response procedures, security measures or operations.

After an assessment or other report of possible breaches of security or security concerns the Ships Security Officer will modify the Plan and report the changes made and the reasons for these changes to the Company Security Officer.

The Ship's Security Officer will immediately report to the Company Security Officer when the effectiveness of security equipment is compromised due to equipment failure or malfunction and will implement operational measures to compensate for the loss of equipment.

The Ship Security Officer will retain all records concerning audit activities.

See Appendix L for example Audit Log.

4.44 Plan Amendments

Upon determination that an amendment to the SSP is needed to maintain the ship's security, the CSO completes the amendment under CEO approval and he forwards it to the ship. As per ISPC A/9.5 and in accordance with the YEN Circular/AA.08 – 01/29.10.2004, whenever following amendments are to be reflected in the SSP, Flag state approval is required. The subject amendments are:

1. Equipment change. Amendment in definition of security levels, restricted areas, access points. Amendment in the ship's and/or company's contacts points

2. Amendment in the ship's security procedures at sea. Above flag state's approval is to be kept with the vessel's ISSC.

4.45 Internal Audits of Company's Security Activities

Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

Completed audit reports should be reviewed by the Company Executives and the CSO. The CSO must submit the audit reports to the Administration along with a list of corrective measures for any deficiencies. The Administration should be advised as soon as possible when all deficiencies are corrected.

SHIP SECURITY ASSESSMENT

4.46 Assessment. A Ship Security Assessment was conducted in accordance with the applicable requirements and it is mentioned here for reference. Appropriate security threats, vulnerabilities and mitigation recommendations have been addressed in this Ship Security Plan as needed and feasible.

The Security assessment survey is a confidential document and will be available as stipulated by the Master in accordance with company policy. A copy of the assessment together with the certificate of the person contacted the SSA can be found attached to this plan.

SHIP ACTIVITIES NOT COVERED BY ISPS CODE

4.47 Port of State which is not a Contracting Government

The ship shall take the following procedure and security measures when it is calling at a port of a State, which is not Contracting Government.

§ Confirm the appropriate competent authority responsible for security of the port or police station with whom the ship shall communicate in an emergency, and establish and maintain the means of communication;

§ Perform the normal protection measures in port;

§ List up the measures not performed in this port out of measures that should be performed if ship is at a port facility of the Contracting Government; and take practicable measures in order to mitigate the security risk that may be caused by none performance of above measures;

- § The SSO shall request and complete the Declaration of Security in order not to leave any doubt, in the future or in next port, about the security measures the ship has taken at this port. If the port facility denied the completion of DoS, enter this fact in the DoS prepared; and,
- § Record the additional measures the ship has performed.

4.48 Interaction with a Ship to which the ISPS Code does not apply

The ship shall take the following procedure and security measures when it has interaction with a ship that flies a flag of a State which is not Contracting Government, or when it is of Contracting Government but is not required to comply with SOLAS XI-2 and ISPS Code.

- § Confirm that another ship does implement the security measures in conformity with other regulations;
- § Confirm that another ship has a security certificate complying with other regulations, and when it has the same, obtain its copy;
- § Perform the normal protection measures for the ship to ship interaction;
- § List up the measures not performed by another ship out of measures that should normally be performed if ISPS Code applied to her; and take practicable measures in order to mitigate the security risk that may be caused by none performance of above measures;
- § The SSO shall request and complete the Declaration of Security in order not to leave any doubt, in the future or in next port, about the security measures the ship has taken at this ship-to-ship interaction. If another ship denied the completion of DoS, enter this fact in the DoS prepared; and,
- § Record the additional measures the ship has performed.

4.49 Interface with a Port Facility to which the ISPS Code does not apply

The ship shall take the following procedure and security measures when the port facility is not required to comply with the ISPS Code, or they have no Port Facility Security Plan.

- § Communicate with competent authority of the Contracting Government;

§ Perform the normal protection measures for ship/port interface;

§ Ship and port shall consult on appropriate security measures, including a request for arrangement of appropriate security measures, and implement the measures as agreed;

§ The SSO shall request and complete the Declaration of Security in order not to leave any doubt, in the future or in next port, about the security measures the ship has taken at this port. If the port facility denied the completion of DoS, enter this fact in the DoS prepared; and

§ Record the measures the ship has implemented.

4.50 Interface with a Platform or MODU

At the interfacing with fixed or floating platforms or mobile drilling unit, the ship shall take the same procedure and security measures as applied to the interface with the port facility not required to comply with the ISPS Code.

CONTINGENCY PLANS AND STANDARD OPERATING PROCEDURES (SOP'S)

Specific scenario-based contingency plans and standard operating procedures may be developed to address identified threats. The following such plans and SOP's are included here as a part of the overall Ship Security Plan. Additional plans and SOP's may be developed when new threats or mitigation methods are established and these will also be included here. SOP’s are only useful if exercised and practiced. The SSO is encouraged to review and practice all SOP’s with the crew.

4.51 Bomb Threats

Objectives	Protect Human Life and Welfare. Notify Master and SSO immediately.	
Tactics	If You Receive a Bomb/Security Threat Attempt to alert someone without stopping the conversation Keep the caller talking (apologize for bad line & ask them to speak up) Complete the checklist listed below as they speak. Try to gain further information. Activate Fire Fighting procedures. Identify any areas downwind that may be affected. Do not hang-up the phone if the call is made from ship's internal telephone system.	
Initial Actions	Activate Alarms.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer.	Contractor Employees:
	Phone Call Particulars	Exact Message Received From Caller
	Date/Time of Call: ____________________ Your Name: ________________________	________________________________ _______________________________ __

About the Caller	Male Female Old Young Accent Speech Impediment Intoxicated Speech	Questions to ask: Where is the bomb? ____________________ What does it look like? __________________ What type of bomb? ____________________ When will it explode? ___________________ How many are there? ___________________ Who else knows about it? _______________
	Background Noise:	Other Information:

Notifications	Name/Title	Contact Numbers	Note/Time Notified

4.52 Evacuation of Ship

Objectives	Protect Human Life and Welfare.

Tactics	General instruction The final decision to abandon ship shall be made by the Master when he believes that this action is imminent after every effort to save the ship has exhausted. It should be reminded that many seamen returned back to ship safely after once abandoned. The master should verify that every measure to save the ship had been taken before abandoning. Nobody should abandon ship until the Master gives clear instruction. It is important to keep the order, accomplish one’s duty and maintain perfect control. At Sea Everybody should follow the Muster List for Abandon Ship. In Port Everybody should assemble in a place pre-designated, and follow instruction given by the PFSO or his/her representative. When there is no such instruction, everybody shall take such action considered necessary to minimize damage to human life, properties and environment.	
Initial Actions	Activate Alarms.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer.	Contractor Employees:
	Date/Time of Evacuation: ________________	Cause of Evacuation: __________________ ________________________________ ___
Life Safety Factors	Evacuation Escape route Blocked	Evacuation Means Lifeboat p Other: _________________
	Muster/Accountability Status: Missing:	Last Known Locations: Confirmed MOB: Entrapment p Visibility/Smoke

	Injured: # Critical: ___ # Delayed: ___ #Minor: ___ # Deceased: ___	Medical Aid: Medics On Scene Medevac by Land/Air

Notifications	Name/Title	Contact Numbers	Note/Time Notified

4.53 Fire

Objectives	Protect Human Life and Welfare. Protect Property and Environment. Activate fire response team.	
Tactics	Activate Shipboard Fire Fighting procedures. Evacuate or shelter personnel not involved in response operations. Contact Specialists to assist with fire fighting.	
Initial Actions	Activate Alarms. Mobilize personnel with proper PPE.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:
	Evacuation Yes p No	Evacuation Means Lifeboat p Other:_________________

	Missing:	Confirmed MOB: Entrapment p Visibility/Smoke	
	Injured: # Critical: ___ # Delayed: ___ #Minor: ___ # Deceased: ___	Medical Aid: Medics On Scene Medevac by Land/Air	
Notifications	Name/Title	Contact Numbers	Note/Time Notified

4.54 Unauthorized Boarding (Piracy)

Objectives	Protect Human Life and Welfare. Protect Property and Environment.

Tactics	When approaching or berthing at a facility in a high-risk area: Minimize access points preferably to a single controlled gangway or ship's side companion way. Keep emergency ladders clear of the water; raise and stow pilot ladders immediately after use. Provide two security officers at access points if a threat warrants the response. Establish perimeter security measures, such as weather deck and ship side lighting, deck and jetty patrols, and secure rat guards on mooring lines. Search all deliveries when possible; conduct frequent, random, and overt searches if all materials cannot be examined. Search all visitors and escort them while on board. Keep small craft in the vicinity under constant surveillance. Carefully control documents containing information about the cargo or ship's itinerary. Conduct a search of the ship before sailing and secure all doors and other access points. Brief crewmembers on the risks of being attacked by pirates or armed bandits. Secure the bridge, engine room, steering gear compartments, officers' cabins, and crew accommodations. Carefully plan any response to an apparent attack and ensure the crew is appropriately trained. If possible, avoid high-risk areas and bottlenecks. Consider delaying ship arrival if there is a high threat from piracy at port and if a berth is not immediately available to minimize the Ship's vulnerability while in queue.	
Initial Actions	Activate Alarms.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:

Life Safety Factors	Evacuation Yes p No	Evacuation Means Lifeboat p Other:___________________
	Muster/Accountability Status: Missing:	Last Known Locations: Confirmed MOB:

Notificatio	Name/Title	Contact Numbers	Note/Time Notified

4.55 Hijacking

Objectives	Protect Human Life and Welfare. Protect Property and Environment.
Tactics	A hijacking is the forcible seizure of a ship by terrorists or pirates. Following are general guidelines in the event of a hijacking: Remain calm and direct crewmembers and passengers to do the same; do not resist armed terrorists or pirates unless there is a clear life-threatening situation. Broadcast a distress message, if possible. The master and crew should not attempt to negotiate with the attackers unless directed. Offer reasonable cooperation; try to establish a basic rapport. Try to identify the number of terrorists or criminals. Attempt to increase the number of access points. Attempt to determine the hijackers' demands and potential deadlines. Use secure communications if available for all discussions with the hijackers. If authorities attempt to regain control of a ship through force, personnel should comply with all commands by military forces. During and after a hijacking, only authorized crewmembers should talk with the media, unless otherwise instructed.

Initi	Activate Alarms.	Accountability Status

	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:

Life Safety Factors	Evacuation Yes p No	Evacuation Means Lifeboat p Other:_________________
	Muster/Accountability Status: Missing:	Last Known Locations: Confirmed MOB:

Notificatio	Name/Title	Contact Numbers	Note/Time Notified

4.56 Damage to Ship (Sabotage) –Attack from seaward

Objectives	Protect Human Life and Welfare. Protect Property and Environment. Activate fire response team.

Tactics	A threat of sabotage, likely to come as a warning that an explosive charge is place on board, will normally be forwarded by letter of telephone. Prompt and organized action is then normally essential. Gather and inform the ship's complement about the situation Initiate an organized a systematic search of the ship Prepare action plans and precautions to limit damages in the event of an explosion, including: Close the connections between all tanks and compartments Close all the water tight doors and all doors in the accommodation Shut down ventilation and close all dampers, skylights and funnel openings Prepare fire fighting and emergency equipment Prepare lifeboats and rafts, if at sea Consider shifting the ship to a more suitable position e.g. port of refuge, protected waters etc. Prepare damage control plan Secure the ship's papers and other important papers Prepare plan for casualty abatement Stay in close liaison with the Company and the local Authorities during the emergency and keep them constantly updated regarding action being executed and attained progress.	
Initial Actions	Activate Alarms.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:
Life Safety Factors	Evacuation Yes p No	Evacuation Means Lifeboat p Other:___________________

	Injured: # Critical: ___ # Delayed: ___ #Minor: ___ # Deceased: ___	Medical Aid: Medics On Scene Medevac by Land/Air	
Notifications	Name/Title	Contact Numbers	Note/Time Notified

4.57 Smuggling

Objectives	Protect Human Life and Welfare.	
Tactics	Precautions to avoid smuggling: Continually look for bubbles coming from the water around the ship’s hull that may indicate divers. Keep close watch on rudder and propeller area and consider the use of turning propeller occasionally. Always be on lookout for suspicious behavior on board ship. Look for evidence of tampering such as damaged bolts, disturbed stowage, closed off spaces, missing keys, etc. Conduct unannounced searches on routine basis. If contraband is discovered: Notify company immediately. Contact local authorities such as Customs. Take photographs of contraband. Use gloves and remove goods to a safe and secure place under guard. Do not open packaging. Do not smoke near object. Make entry into log book on discovery and actions taken.	
Initial	Contact Local Customs	Accountability Status

<table>
<tr><td rowspan="2">🟥</td><td colspan="2">Contact Local Emergency Services.</td><td>Company
Employees:</td></tr>
<tr><td colspan="2">Contact Company Security Officer</td><td>Contractor
Employees:</td></tr>
<tr><td rowspan="2">Notifications</td><td>Name/Title</td><td>Contact Numbers</td><td>Note/Time Notified</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

4.58 Stowaways

<table>
<tr><td>Objectives</td><td colspan="3">Protect Human Life and Welfare.
Protect Property and Environment.</td></tr>
<tr><td>Tactics</td><td colspan="3">When a stowaway is found, the master shall immediately inspect this person.
In order to identify this person, the ship shall collect as much document as possible pertaining to him such as passport, seamen’s note, ID card, physical check record, letters, etc.
In general, a stowaway denies his possession of document, and uses a false name and false nationality. However, in many cases, the stowaways hold their identity paper in secret, near the compartment where they were found. Therefore, the ship should perform a systematic search of document.
Most important action at finding of stowaway is to report to the company, immediately, of this fact together with all information available.
Also report to the authority and agent where the stowaway came onboard, and to the same of next port.
Refrain from raising uproar for the stowaway. But give him a room and meal.
During navigation along coastal water and in port, keep him calm in a locked room, and avoid unnecessary contact of crewmember with him, until further instruction is issued.
In general, ship’s deviation just for disembarkation of the stowaway is not permitted in the charter party. He shall be disembarked only after approval of the company.</td></tr>
<tr><td rowspan="3">Initial Actions</td><td colspan="2">Mobilize personnel to deal with Stowaway(s).</td><td>Accountability Status</td></tr>
<tr><td colspan="2">Contact Local Emergency Services.</td><td>Company
Employees:</td></tr>
<tr><td colspan="2">Contact Company Security Officer</td><td>Contractor
Employees:</td></tr>
<tr><td>Notif
ation</td><td>Name/Title</td><td>Contact Numbers</td><td>Note/Time Notified</td></tr>
</table>

🟨			

4.59 Hostage Taking

Objectives	Protect Human Life and Welfare.	
Tactics	Hostage taking is the forcible seizure of personnel by terrorists. Following are general guidelines in the event of a hostage taking incident: Remain calm and direct crewmembers and passengers to do the same; do not resist armed terrorists unless there is a clear life-threatening situation. Broadcast a distress message, if possible. The master and crew should not attempt to negotiate with the attackers unless directed. Offer reasonable cooperation; try to establish a basic rapport. Try to identify the number of terrorists or criminals. Attempt to increase the number of access points. Attempt to determine the terrorists' demands and potential deadlines. Use secure communications if available for all discussions with the terrorists. If authorities attempt to regain control of a ship through force, personnel should comply with all commands by military forces. During and after a hostage taking, only authorized crewmembers should talk with the media, unless otherwise instructed.	
Initial Actions	Activate Alarms, if feasible and not life threatening.	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:
Life Safety	Evacuation Yes **p** No	Evacuation Means Lifeboat **p** Other:________________

🟩	Injured: # Critical: ___ # Delayed: ___ #Minor: ___ # Deceased: ___		Medical Aid: Medics On Scene Medevac by Land/Air
Notific tions	Name/Title	Contact Numbers	Note/Time Notified

4.60 Search of Ship

Objectives	Protect Human Life and Welfare. Protect Property and Environment.		
Tactics	A search should be organized based on a search plan that is specific to the ship, which may direct the crew to use specific external assistance. Use of diagrams, etc, will help facilitate areas to be searched on board the ship. Searchers should be familiar with the search areas so they can identify new or unusual items. Officers and management should carefully supervise the search. Consideration should be given to search parties working in pairs, with one person searching “high” and the other one searching “low.” Searchers should be aware that bombs could come in a variety of shapes and sizes. Anything out of the ordinary should be noted and reported. Areas that have been searched should be appropriately marked. A central point of contact should be established to coordinate information. Searchers should have communication devices so they can alert officers and management. Searchers should be trained so they know what to do if a bomb is discovered. If a bomb is located, the search should continue in case another device is present.		
Initial Actions	Activate Alarms if necessary.	Accountability Status	
	Contact Local Emergency Services.	Company Employees:	
	Contact Company Security Officer	Contractor Employees:	
Notificatio	Name/Title	Contact Numbers	Note/Time Notified

4.61 Use of Ship as Weapon

Objectives	Protect Human Life and Welfare. Protect Property and Environment.		
Tactics	There are many ways a ship can be used as a weapon. It can be used to ram another ship, or an offshore or shore facility. The ship could have an explosive device planted on board that may be detonated by persons on board or remotely. In any case, whatever the scenario, other SOP's, such as *Hijacking, Bomb Threat, or Search of Ship*, contained herein, or in other shipboard manuals will likely provide the needed guidance. As with other SOP's the following are guidance's for handling the situation: Remain calm Attempt for obtain as much information as possible If possible, notify local authorities Evacuate all non-essential personnel		
Initial Actions	Activate Alarms.	Accountability Status	
	Contact Local Emergency Services.	Company Employees:	
	Contact Company Security Officer	Contractor Employees:	
Life Safety Factors	Evacuation Yes p No	Evacuation Means Lifeboat p Other:___________________	
	Muster/Accountability Status: Missing:	Last Known Locations: Confirmed MOB:	
Notificatio	Name/Title	Contact Numbers	Note/Time Notified

4.62 Weapons on Board and Suspicious Objects

Objectives	Protect Human Life and Welfare. Protect Property and Environment.
Tactics	It is the policy of this company and this ship that the possessions of firearms on board the ship is prohibited except for those government agents and duly authorized private security guards. All other weapons, knives, clubs, etc., shall be subject to the following procedure: If a weapon is discovered in the possession of anyone, other than listed above the Master or SSO will: Refuse access to the ship of the person possessing the weapon or Take possession of the weapon and return it to the owner when he/she disembarks from the ship. It is recommended that if at all possible the person possessing a weapon be requested to secure the weapon off premises of the ship prior to boarding. Obviously the definition of a weapon may be very broad and the Master should consider the safety of the crew in defining what is a weapon and what is not.

Initial Actions	Immediate Notifications	Accountability Status
	Contact Local Emergency Services.	Company Employees:
	Contact Company Security Officer	Contractor Employees:

Notificatio	Name/Title	Contact Numbers	Note/Time Notified

APPENDIX (A) COMPANY CONTACT INFORMATION

24 Hours Contact Number: + …………

Security e-mail: security.alert@

Company Security Officer One of the below numbers must be a 24 hour contact number	
Name	
Company Address	Y Shipping Co. Ltd GR, Athens Greece
Business Phone	+30 ……….
Fax	+30 …………
Residence	+30 …………….
Mobile-**24 hour**	+30 …………..
Email	………@.........gr
Alternate Company Security Officer	
Name	………..
Company Address	Y Shipping Co. Ltd GR-, Athens, Greece
Business Phone	+30 ……….
Fax	+30 ………..
Residence	+30 ……..
Mobile – 24 hours	+30 ……..
Email	…@........gr

Company may name and additional officers.

OOPS Qualified Individual

Name	Mr……..
Company Address	OOPS ……………..
Business Phone	+ 1 ………..
Fax	+ 1 …………
Mobile-24 hours	+ 1 …………..
Email	security.alert@……… com (EMERGENCY 24 HOURS)

Kindly note that Security notifications should be made in the order given above until a company representative is contacted. Only the persons above are authorized to receive a security report.

APPENDIX (B) INTERNATIONAL SHIP SECURITY CERTIFICATE

Original is to be kept in Classification and Trading Certificates file. As per the SMSM Ch.3 Technical department has to monitor and ensure that the vessels certificates are always kept updated through the electronic data program. When the ISPC interim or renewal inspection is due to be carried out the Technical department has to inform the CSO and the alternates CSOs who are responsible to make the necessary arrangements for the prompt inspection of the vessel.

Further more and in accordance to the SMSM Ch. 5, the Master is also responsible to ensure that the vessel's certificates are kept always updated and to inform the office when a certificate is due to expire.

APPENDIX (C) CONTRACTING GOVERNMENT EMERGENCY CONTACTS

COUNTRY	AGENCY	CONTACT INFORMATION

APPENDIX (D) INVENTORY OF DANGEROUS GOODS OR HAZARDOUS SUBSTANCES

Voyage Number:				
Kind	Quantity	Stowage Place	Inspection Date	Person In Charge of Inspection

APPENDIX (E) BUSINESS MANAGEMENT FORM

	Division Name, Etc.	Contact Point and Phone
Parties responsible for appointing shipboard personnel. (B/6.1.1)	Crewing Department	…..Tel: +30 mobile
Parties responsible for deciding bareboat charterer(s). (B/6.1.2)	Operations Department	…..Tel: + 30 ….Mr Tel: +44………..
Parties responsible for deciding time charterer(s). (B/6.1.2)	Operations Department	Mr…… Tel: + 30 210 …..Mr.. Tel: +44……..

Parties responsible for deciding voyage charterer(s). (B/6.1.3)	Operations Department	Mr…. Tel: + 30 210 Mr… Tel: +44…………
* Note: Master is to follow instructions, in respect to the charter party, posted only from operations department (Mr so and so). Should they ever receive any other information/instruction they should re confirm the validity with the operations department.		

CEO

Friday, xxx 2003. Signed.

APPENDIX (F) SECURITY INCIDENT REPORT

a. SHIP OR PORT AREA DESCRIPTION

Name of Ship: ____Flag: ____________

Master**:** _____________________Port Facility Security Officer: _________________

Ship Security Officer: _________________________

b. BRIEF DESCRIPTION OF INCIDENT OR THREAT

____

____

c. DATE, TIME, AND PLACE (Lat/Long) OF INCIDENT OR THREAT:

____

d. NUMBER OF ALLEGED OFFENDER (S)

Crew: _________________________Other:_________________________________

e. DETAILS OF OFFENDER (S)

Name:	Nationality:	DOB/POB

f. NUMBER OF ALLEGED VICTIM (S)

Crew: ______________________Other:_____________________________

g. DETAILS OF VICTIM (S)

Name:	Nationality:	DOB/POB

h. NATURES AND SEVERITY OF INJURY SUSTAINED

Name	Injury

i. TYPE OF DANGEROUS SUBSTANCES OR DEVICES USED (FULL DESCRIPTION)

Weapon: ____

Explosives: ____

Other: ____

j. METHOD USED TO INTRODUCE DANGEROUS SUBSTANCES OR DEVICES INTO THE PORT FACILITY OR SHIP

Persons: ____

Baggage: ____

Cargo: ____

Ship Stores: ____

Other: ____

(a) Where were the devices/items described concealed?

____

(b) How was the security measures circumvented?

____

k. WHAT MEASURES AND PROCEDURES ARE RECOMMENDED TO PREVENT A RECURRENCE OF A SIMILAR EVENT?

____

l. OTHER PERTINENT DETAILS (Use additional sheets if required)

____

m. Upon receipt of a security incident report, the CSO files a written report of said incident, to the appropriate authorities.

APPENDIX (G) SECURITY LEVELS OF LAST 10 PORTS

Voyage No.	Name of Port	Arrival Date	Departure Date	Security Level		Special Measures Taken
				Port	Ship	

APPENDIX (H) SECURITY TRAINING SCHEDULE

Security Training Schedule			
Item	Involving	Frequency	Comments
Training Sessions			

Security Training Schedule			
Item	Involving	Frequency	Comments
Initial Security Awareness Training	Entire ship crew	During Familiarization training	
Security Plan Training	Selected Crew members	When assigned. Also when the plan is revised	Should include all personnel who have a role in implementing any action in the security plan
Ship Security Officer Training	All personnel that will assume the role of SSO	Prior to assignment	Should cover regulatory basis for and development/ Maintenance of security plans
Ship Security Officer Training	All personnel that will assume the role of SSO	Every 5 Years	Should cover regulatory basis for and development/ Maintenance of security plans
Security equipment	Personnel assigned to use the equipment	Prior to assignment	May be adequate implement manufacturer provided procedures and training

APPENDIX (I) DRILL AND EXERCISE SCHEDULE

The drills and exercises are to be conducted following the attached Company's Annual Drill Program. The scenarios, list of participants and the evaluations of the drills/exercises are to be sent to the attention of the CSO. During the SSA tests/exercises the SSO shall be contacted directly by the CSOs and/or alternates CSO and the OOPS QI (Kline Calvin) to confirm the test performance.

APPENDIX (J) SSO

PORT SECURITY SURVEY

The following checklist identifies potential vulnerabilities in security measures and procedures at port facilities:

Voyage Number: ____________________

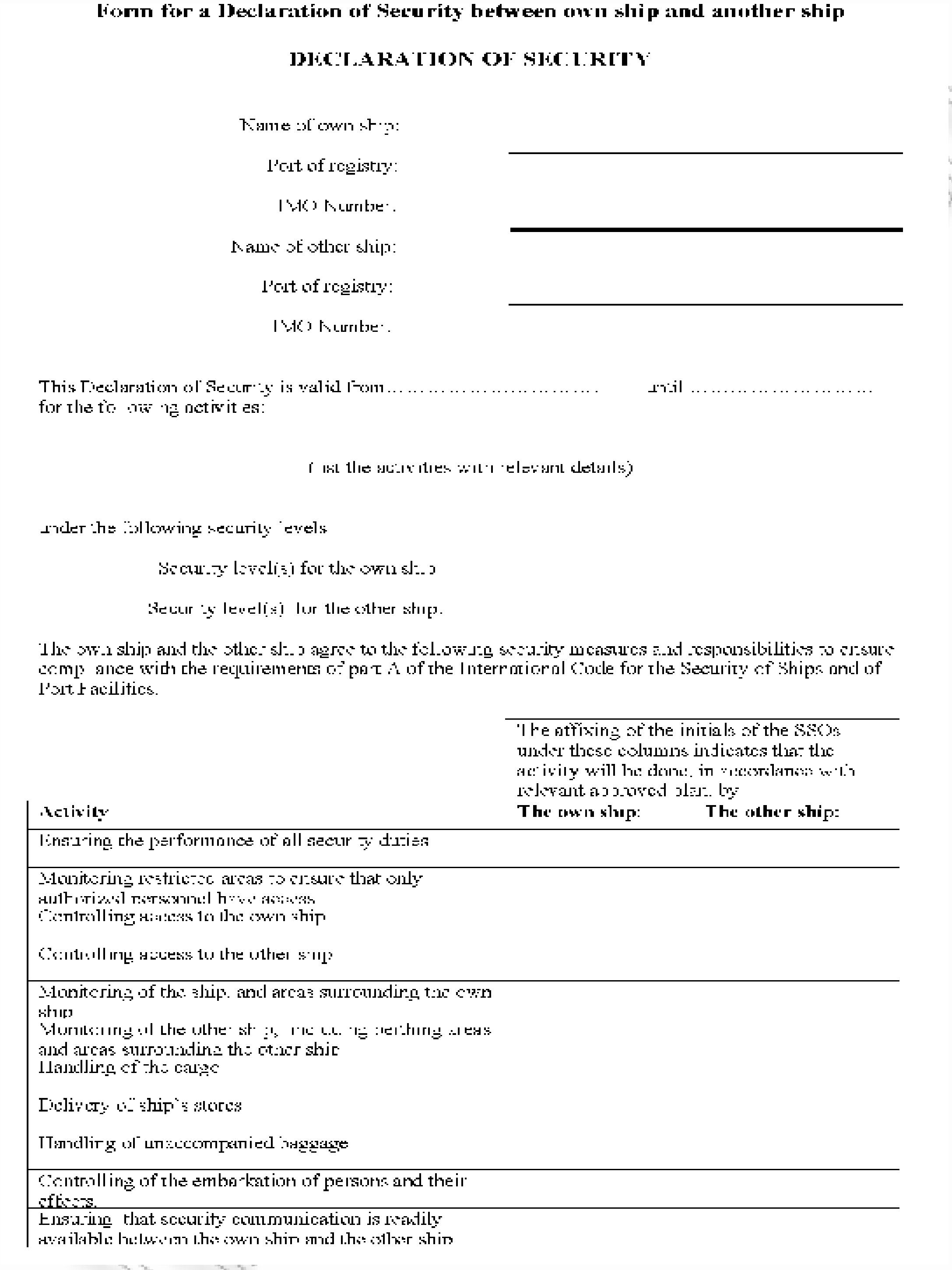
Date/Time:_______________

Yes	No	The port facility has conducted a security assessment? If yes, when?
Yes	No	Are Inspection, control, and monitoring systems and procedures followed appropriately?
Yes	No	Identification documents?
Yes	No	Are Access control systems and procedures (including checking of ID''s) followed?
Yes	No	Perimeter security measures (fencing, etc.)?
Yes	No	Is Lighting adequate?
Yes	No	Are personnel sufficient to respond to an emergency?
Yes	No	Are Communication means adequate?

If answered No to any question, please explain:……………………………………

Deficiencies in the Port Facility Security should be reported to the Company Security Officer and the Flag Administration. Serious deficiencies should be reported by the quickest means possible: telephone, fax or E-Mail.

APPENDIX (K) DECLARATION OF SECURITY FORM



Form for a Declaration of Security between own ship and another ship

DECLARATION OF SECURITY

Name of own ship:

Port of registry:

IMO Number:

Name of other ship:

Port of registry:

IMO Number:

This Declaration of Security is valid from…………………………… until ……………………… for the following activities:

(list the activities with relevant details)

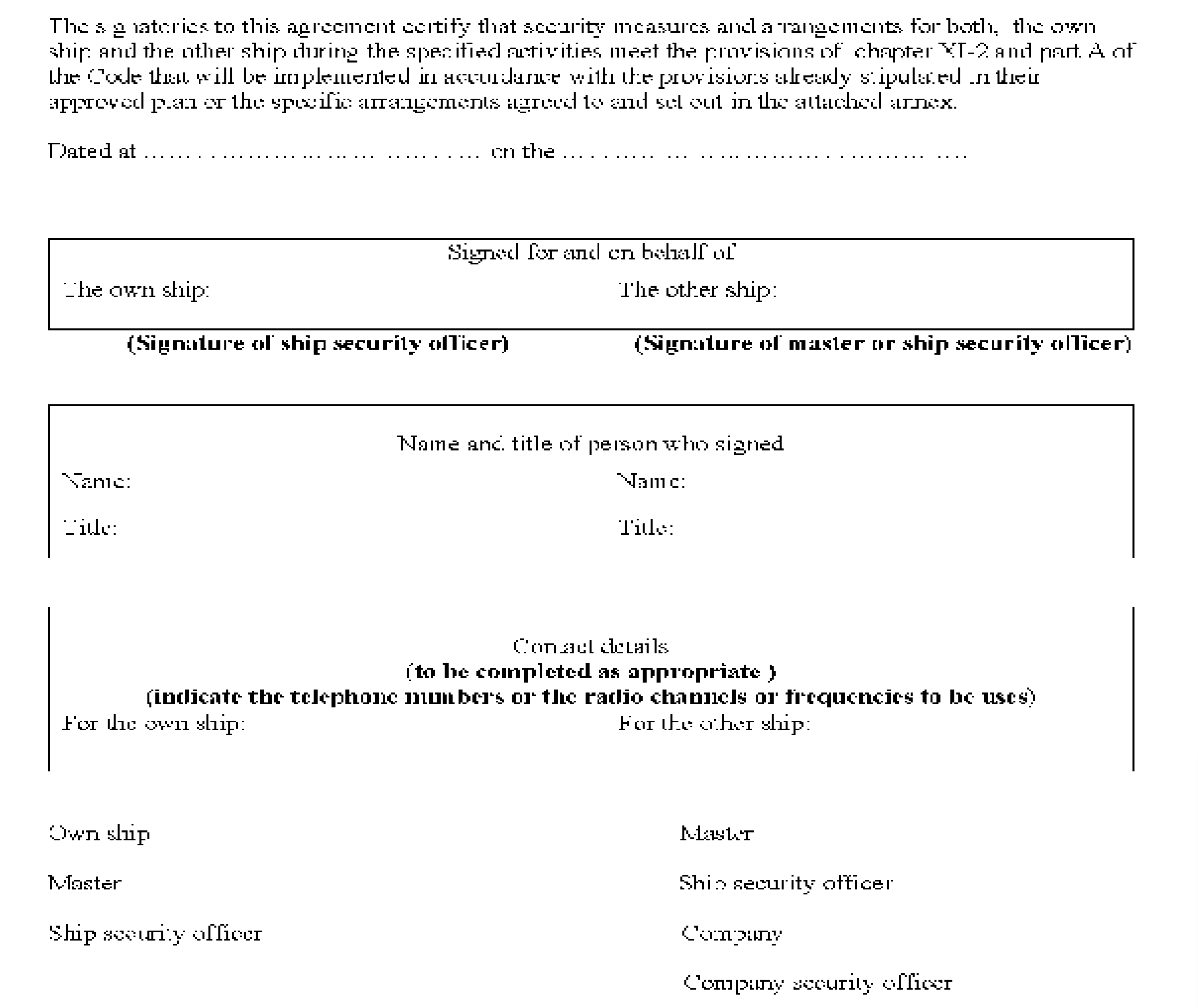
under the following security levels

Security level(s) for the own ship

Security level(s) for the other ship:

The own ship and the other ship agree to the following security measures and responsibilities to ensure compliance with the requirements of part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSOs under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	**The own ship:**	**The other ship:**
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access Controlling access to the own ship Controlling access to the other ship		
Monitoring of the ship, and areas surrounding the own ship Monitoring of the other ship, including berthing areas and areas surrounding the other ship Handling of the cargo Delivery of ship's stores Handling of unaccompanied baggage		
Controlling of the embarkation of persons and their effects.		
Ensuring that security communication is readily available between the own ship and the other ship		



The signatories to this agreement certify that security measures and arrangements for both, the own ship and the other ship during the specified activities meet the provisions of chapter XI-2 and part A of the Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at …………………………………… on the ……………………………………………

Signed for and on behalf of

The own ship:	The other ship:
(Signature of ship security officer)	**(Signature of master or ship security officer)**

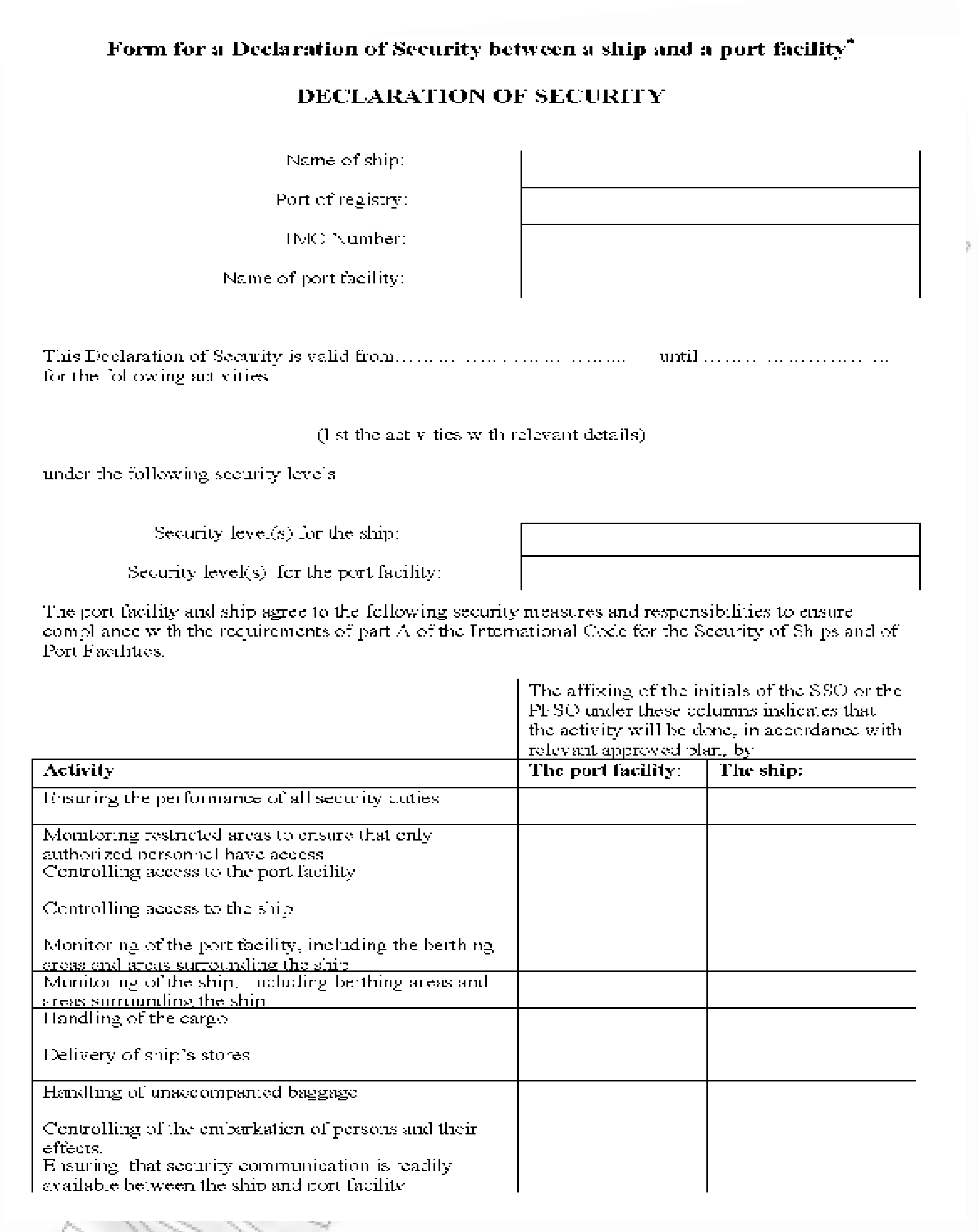
Name and title of person who signed

Name:	Name:
Title:	Title:

Contact details
(to be completed as appropriate)
(indicate the telephone numbers or the radio channels or frequencies to be uses)

For the own ship:	For the other ship:

Own ship	Master
Master	Ship security officer
Ship security officer	Company
	Company security officer



Form for a Declaration of Security between a ship and a port facility*

DECLARATION OF SECURITY

Name of ship:	
Port of registry:	
IMO Number:	
Name of port facility:	

This Declaration of Security is valid from………………………………… until ……………………… for the following activities

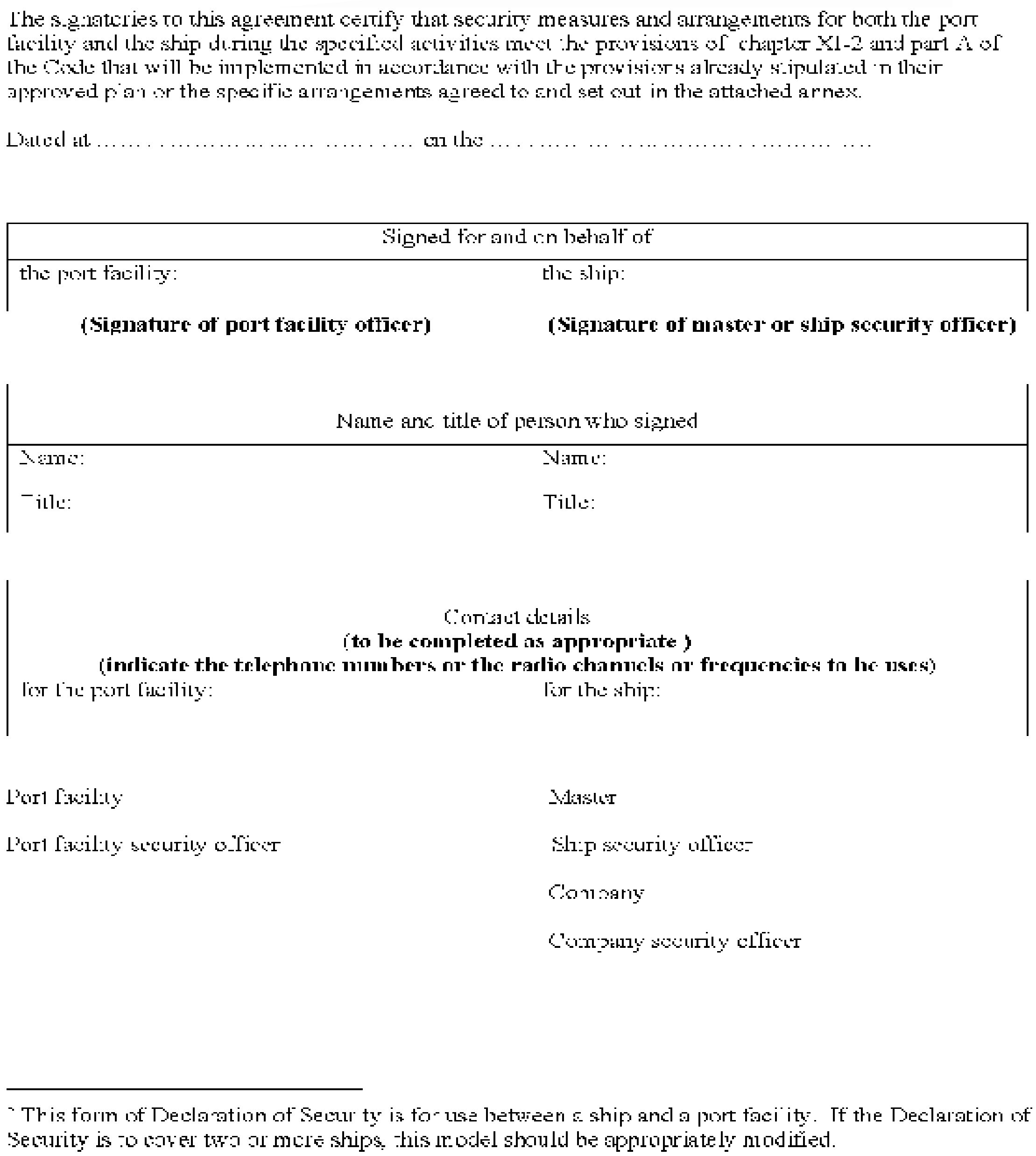
(list the activities with relevant details)

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or the PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	**The port facility:**	**The ship:**
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access Controlling access to the port facility Controlling access to the ship Monitoring of the port facility, including the berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of the cargo Delivery of ship's stores		
Handling of unaccompanied baggage Controlling of the embarkation of persons and their effects. Ensuring that security communication is readily available between the ship and port facility		



The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and part A of the Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at …………………………………… on the ………………………………………

Signed for and on behalf of	
the port facility:	the ship:
(Signature of port facility officer)	**(Signature of master or ship security officer)**

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

Contact details **(to be completed as appropriate)** **(indicate the telephone numbers or the radio channels or frequencies to be uses)**	
for the port facility:	for the ship:

Port facility	Master
Port facility security officer	Ship security officer
	Company
	Company security officer

[1] This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two or more ships, this model should be appropriately modified.

APPENDIX (L) AUDIT LOG

Audit Description	Findings	Response	Resolution Date	CSO/ Signature

APPENDIX (M)

COMPANY SECURITY OFFICER DESIGNATION & ALTERNATES CSOs

INTERNAL MEMO

To: All Ship Masters

All department heads

From: CEO

Subject: COMPANY SECURITY OFFICER & ALTERNATES CSOs DESIGNATION

Captain Mr… is hereby designated as the primary Company Security Officer (CSO) and Mr …and Mr… & Miss… as alternates CSOs. This appointment is effective 11 April 2007.

In this role, CSO and his delegates will have the following primary responsibilities:

- Coordinating and overseeing the overall company security program;
- Monitoring and advising regarding security threats which may be encountered by the ship(s);
- Ensuring that ship security assessments and annual reassessments are carried out;
- Developing and maintaining the Ship Security Plan(s);
- Ensuring adequate training for personnel with security responsibilities;
- Coordinating and communicating with Ship Security Officer(s);
- Auditing compliance with security plans and procedures, and implementing corrective actions as required; and
- Enhancing security awareness and vigilance.

Company personnel are instructed to cooperate with and assist the CSO in the commission of these duties.

CEO à signed

APPENDIX (N) SHIP SECURITY OFFICER DESIGNATION

INTERNAL MEMO

To: All Ship Masters

All department heads

From: CEO

Subject: SHIP SECURITY OFFICER DESIGNATION

The Master is hereby designated as the Ship Security Officer (SSO) for the M.T xxxx and Chief Officer as his deputy.This appointment is effective 23 May 2007.

In the role of the SSO, the Master will have the following primary responsibilities:

- Coordinating and overseeing the ship security program;
- Monitoring and advising regarding security threats which may be encountered by the ship;
- Implementing and maintaining the Ship Security Plan and proposing changes to the plan;
- Conducting regular security inspections of the ship;
- Ensuring adequate training for ship personnel with security responsibilities;
- Coordinating with the Company Security Officer;
- Ensuring that security equipment onboard the ship is operating properly and maintained;
- Enhancing security awareness and vigilance onboard; and
- Completing Declaration of Security agreements and coordinating with waterfront facilities.

Company and ship personnel are instructed to cooperate with and assist the SSO in the commission of these duties.

CEO à signed.

APPENDIX (O) SHIP SECURITY EQUIPMENT MAINTENANCE

(See attached F075 included in Vessel’s Forms)

APPENDIX (P)

PROCEDURE FOR RESETTING SHIP SECURITY ALERT

1. Go to www……finder.com . Enter User name company Y. Enter Password xxxxx. Right-click on the vessel you want to reset. Go to Communication window. Pick the vessel you want to reset. Communication window then opens writing the name of the vessel you picked. Go to Special and pick Reset Panic Button. Then press Send. Wait for approximately 5 minutes till command has been given. Close …… finder.

APPENDIX (Q) FLAG STATE NOTIFICATION

Please find attached the Contact details of the Ministry of Mercantile Marine Joint Rescue Coordination Center in Piraeus, which should be notified by CSO or his delegates or OOPS (Mr so and so) under the case that Ship Security Alert is being activated and a real threat is being identified on board. The following contacts are the proper recipients of SSAS as they have been released by IMO.

IMO Global Integrated Shipping Information System (GISIS)

View Details à Contact type: Proper recipients of SSAS alerts

Country of contact: Greece.

Name of Organization/Authority/Department**:** Ministry of Mercantile Marine Joint Rescue Coordination Center Piraeus (JRCCP)

First name: **-** Surname: **-** Title: H.C.G. Officer Contact post: Officer on duty

Specific responsibilities: **--** Conditions of authority**:** --

Address line 1**:** 150, Gr.Lampraki Str., 18518 Piraeus, GREECE Address line 2: --

Address line 3: **--**Postcode**:** 18518 Fax**:** +30 210 4132398 Mobile:**-**

Phone**s:** +30 210 4191369, 4112500, 4191703, 4191704, 4191379, 4220772, 4111061

Telex: +601-211588, 211254 **Email:** Jrccpgr@.yen.gr , cc: dedaple@.yen.gr, **Website:** --

APPENDIX (R) FLAG STATE CIRCULARS

Below are listed the Greek Flag circulars which are mentioned in the subject manual. All relevant circulars are sent on board as a Security alert/ Bulletin.

YEN Circular / 3725.1/123/05 / 19-07-2005 YEN/ΚΝΠ/ΔΕΔΑΠΛΕ Β΄ - *Γ΄*