

A joint project by:



# GUIDE FOR TANKERS OPERATING IN ASIA AGAINST PIRACY AND ARMED ROBBERY INVOLVING OIL CARGO THEFT





#### ACKNOWLEDGEMENT

This guide was produced by the ReCAAP ISC in collaboration with the S. Rajaratnam School of International Studies (RSIS) and the Information Fusion Centre (IFC), in the desire to promote safe and secure seas for the shipping community. We express our gratitude to the RSIS for writing the guide, to RSIS, IFC, shipping companies, regional and international shipping associations, likeminded entities and individuals who had contributed their views and ideas in making this guide a credible and reliable source of reference.

# CONTENTS

Section 1	Introduction	1
Section 2	Threats To Mariners	2
Section 3	Principal Risk Factors And Mitigation Measures	3
Section 4	Maritime Security Planning Considerations	11
Section 5	Ship Protection Measures	14
Section 6	Ships Under Attack	19
Section 7	Role Of Mariner In Improving Situation In Asia	20
Section 8	Post-Incident Reporting And Follow-Up	22
Annex A	Definitions	23
Annex B	Reporting Format	24
Annex C	Contact Details	25
Annex D	Voluntary Community Reporting	29
Annex E	Partner Organisations	33

# SECTION 1

## INTRODUCTION

---

The aim of this guide is to illustrate the threat of piracy and armed robbery against ships (hereafter referred to as 'sea robbery') in Asia, particularly incidents involving oil cargo theft; and to assist ships to avoid, deter or delay such incidents; as well as post-incident management. This continued occurrence of oil cargo theft incidents warrants the need to produce a "*Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft*". The definition of 'piracy' (in accordance with UNCLOS) and 'armed robbery against ships' (in accordance with IMO) can be found in Annex A.

This guide serves as a prelude to a regional guide on piracy and armed robbery against ships which will be published in due course. The regional guide will take into consideration the occurrence of incidents involving all types of ship while underway and at ports and anchorages in Asian waters. That being said, until the publication of the planned regional guide, it is noted that some if not all of the recommendations made in this Guide can potentially be applicable to other types of ships.

## SECTION 2

# THREATS TO MARINERS

---

In 2014, the ReCAAP ISC published a Special Report on “Incidents of Siphoning of Fuel/Oil at Sea in Asia”, highlighting its concern over the increase in the number of such incidents in Asia. Notably, one incident was reported in 2011, four in 2012, three in 2013, and 15 in 2014.

In 2015, the ReCAAP ISC published Part II of the Special Report on “Incidents of Siphoning of Fuel/Oil at Sea in Asia”, highlighting worrisome trends since 2014, focusing on the modus operandi of the perpetrators and highlighting possibility of the involvement of syndicates and organized groups. Of particular note in Part II of the Special Report is the observation that, of the 15 oil cargo thefts reported in 2014, two-thirds involved tankers of less than 3000 Gross Tonnage (GT). Of the 15 cases, eight involved tankers of 1000-2000 GT, two involved tankers of 2000-3000 GT, four incidents involved tankers of 3000-4000 GT and one involved tanker of > 5000 GT.

For the first nine months of 2015, a total of 12 incidents had been reported; of which two incidents were foiled by the authorities whose timely responses to the immediate reporting by the masters and shipping companies had resulted in the arrest of the perpetrators involved. Between 2011 and September 2015, a total of 35 oil cargo theft incidents had been reported in Asia with more than half of them occurring in the South China Sea.

## SECTION 3

# PRINCIPAL RISK FACTORS AND MITIGATION MEASURES

Before beginning a voyage, a thorough risk assessment should be carried out; among others, to examine the likelihood and consequences of the ship being robbed, pirated or even hijacked; as well as to identify the appropriate measures for prevention, mitigation, reporting and recovery.

To aid in the risk assessment, the planner should understand the general situation of piracy and sea robbery in the region taking into consideration factors contributing to certain trends, locations that are more vulnerable for piracy and sea robbery, type of ships that are targeted more often, type of cargo that are much sought after, modus operandi of perpetrators involved in particular type of attack, etc. Such knowledge and situation awareness will enable the planner to develop appropriate countermeasures, adopt necessary mitigation responses, identify the relevant reporting channels and procedures, and establish post incident management including recovery and evidence preservation.

### 3.1 Contributing Factors

The frequency of ship hijacking for oil cargo theft continues to escalate since 2014. There are several factors that account for the rising occurrence of these incidents.

- A) The accessibility of seaborne shipping which inadvertently generated significant numbers of slow-moving, isolated and lucrative targets which perpetrators are seeking.
- B) Technological advances have resulted in improved ship-operating efficiencies that reduce the size of the crew, enable perpetrators to track the position, speed, voyage, and information about the cargo carried on board the targeted ship. The accessibility of such data through internet and live portals permits 'interested parties' to obtain up-to-date information about ships that were targeted.
- C) Taking advantage of the fall in global oil prices, the industry is making bulk purchase of oil for stockpiling purposes, and this resulted in increased traffic by tankers especially in regional waters to meet the demand for cheaper oil.
- B) Other factors include: demand for cheaper oil by smaller boats and fishing vessels, fluctuating market price of oil, availability of potential buyers scouting for cheaper oil, presence of black markets for buying and selling of stolen oil, and difficulty in tracing the origin or source of the oil to facilitate prosecution for theft. The porous nature of the maritime environment, particularly areas with high volumes of sea traffic may constitute another possible factor.

### 3.2 Incident Locations, Type of Vessel, Gross Tonnage and Type of Cargo

More than half of the oil cargo thefts in Southeast Asian waters occurred in the South China Sea (SCS) where significant sea traffic volumes are observed daily. To avoid being detected by enforcement agencies, the perpetrators usually steer the hijacked ship further away from shore to carry out siphoning of the oil cargo on board. This makes enforcement by naval and maritime agencies; and maintenance of regular presence in these areas more challenging. This explains why such incidents have become more prevalent in and throughout the region especially in the SCS.

Based on reports on incidents of oil cargo theft in Asian region during 2011 – September 2015, product/oil tankers of less than 5000 GT carrying Marine Gas Oil (MGO) had been targeted more frequently, and majority occurred in the SCS. The observed trends of these incidents are summarized in Table 1 below.

**Table 1: Classification of Oil Cargo Thefts in Southeast Asian Waters 2011- Sep 2015**

Category	Sub-Categories	Number
Incident Location	South China Sea	21
	Straits of Malacca and Singapore	6
	Others	8
Type of Vessel	Product /Oil Tanker	24
	Tanker	6
	Chemical Tanker	2
	Bunker Tanker	2
	Supply Vessel	1
Gross Tonnage	<2000 GT	20
	2000-5000 GT	9
	>5000 GT	4
	Not known	2

Category	Sub-Categories	Number
Type of Cargo (1)	Marine Gas Oil (MGO)	9
	Diesel	4
	Marine Fuel Oil (MFO)	4
	Fuel Oil	2
	Gasoline	2
	Gas Oil	2
	Hot Asphalt	1
	Lube Oil	1
	Marine Diesel Oil (MDO)	1
	Automotive Diesel Fuel (ADF)	1
	Diesel and Bulker Oil	1
	Palm Oil	1
	Petrol	1
	Petrol and Diesel	1
	Not known	4

(1) As reported without further categorisation

### 3.4 Operations and Trends

The number of incidents reported during 2011-September 2015 involving hijacking of tankers for theft of the oil cargoes carried on board have been of significant concern to the regional maritime commerce. Based on the information about these incidents, the nature of the perpetrators, their modus operandi, knowledge and accessibility of information on the industry processes are as outlined below.

#### (A) Organised Groups and Syndicates

From the arrest made by the Singapore Police Coast Guard in September 2014, the 53 men apprehended were believed to be involved in illegal ship fuel trade and operated in syndicates comprising the mastermind and middle-men who served as the go-between for buyers and sellers. Based on information provided by crew regarding the modus operandi of perpetrators involved in incidents reported since 2011 till present, the ReCAAP ISC and its operational partners believed these syndicates operate in similar modality of having mastermind and middle-men; and there are at least three organised groups or syndicates involved, each operating in different locations of these incidents in the SCS and the Malacca Strait.

## **(B) Modus Operandi**

Generally, the modus operandi of the perpetrators in most of the oil cargo thefts is fairly similar. They usually board the victim ship during hours of darkness, tie or lock-up the crew, take control of the ship and steer her further away from shore, order one of the crew to open the valve and siphon the oil cargo into another tanker or barge that comes alongside the victim ship. Before leaving the ship, the perpetrators will steal the crew's cash and personal belongings and destroy the ship's communication and navigation equipment to delay the crew from reporting to the authorities.

In most cases, the target was the oil cargo on board the hijacked ship; however, there were a few cases where the perpetrators opted to not just board the ship and unload the cargo, but hijacked the ship with its cargo intact and repainted it to avoid detection. Whether or not they have any plan to sell the ship and its cargo remains unknown. However, thus far there has been no evidence that the ship was intended to be sold. In all cases investigated so far, the oil cargo was the target.

It was unusual in one incident where the ship was hijacked for a few days while some of the perpetrators left the ship to look for buyer. In majority of the incidents, the perpetrators would have had readily-available buyers. The ReCAAP ISC believes that this could be an issue of 'intelligence' failure as to the type of oil cargo the perpetrators were looking for. This explains the situation in some incidents where the perpetrators left the ship without theft of the oil cargo after discovering that it was not the type that they wanted, or demanded in the black market.

## **(C) Knowledge and Accessibility of Information on Industry Processes**

From description of the incidents, it is believed that the syndicates and organised groups would have good knowledge and accessibility of information on the industry processes, such as:

- Type of oil cargo carried by the victim ship;
- Route undertaken;
- Type of equipment on board the ship to facilitate the siphoning process;
- Preferred location for the siphoning operation to avoid detection by authorities;
- Scheduling of another tanker/barge to come alongside the ship at specific time and location;
- Storage of the siphoned oil cargo and the location to transfer it to potential buyers;
- Type and grade of oil on demand;
- Market knowledge on the availability of cheap oil among buyers and sellers, and such information is normally transmitted through word of mouth;
- Knowledge of the supply chain process.

### 3.5 Generic Risk Assessment

Table 2 presents generic risk assessment based on past available information of the 35 incidents during the period of 2011 till September 2015. The level of risk exposure is defined here as the likelihood of an incident that may occur to the tanker, and is categorised as low, medium and high. For the purpose of this table, parameters used to derive the level of risk are the tanker's, gross tonnage, type of oil cargo carried and location. The mitigation measures are differentiated according to the assessed risk exposure.

It needs to be noted that Table 2 only presents a tentative form of risk assessment based on the patterns of incidents observed thus far. The parameters of this assessment may be adjusted in order to keep in pace with how the future situation evolves.

**Table 2: Generic Risk Assessment Table**

Risk		Low	Medium	High
Gross Tonnage	< 2000			x
	2000 - 5000		x	
	> 5000	x		
Type of Oil Cargo	MGO, MFO, MDO, Diesel, ADF			x
	Gasoline, lube oil, palm oil and others		x	
	Others (e.g. hot asphalt)	x		
Location	South China Sea			x
	Malacca Straits	x		
	Other Locations		x	
Possible Mitigation Measures		Comms RSL/TSS	Comms RSL/TSS SPM	Comms RSL/TSS SPM TID

#### Legend

Comms	Maintain communications with littoral States
RSL/TSS	Transit within Recognised Shipping Lanes/Traffic Separation Schemes
SPM	Implement appropriate Ship Protection Measures
TID	Transit during daylight hours through vulnerable areas

### 3.6 Preventive Measures

Training of crew on anti-piracy drills and evidences preservation is critically important and strongly recommended. Also CSO and ship master should ensure that there is a proper ship security plan in place. This includes the installation of ship protection measures (SPMs), screening of crew, conduct of crew briefing/training, proper planning of voyage by avoiding vulnerable areas, if possible, maintaining confidentiality of the voyage route, as well as defining the AIS, reporting procedures and policies, etc.; prior to the start of the voyage.

There is no better way to address the problem of piracy and sea robbery other than to be ready, prepared and equipped before being confronted with it. Ship owners and CSOs must continually review their ship security plans and standard operating procedures by keeping abreast of the latest situation in the region, especially the vulnerable areas.

After considering the modus operandi adopted by perpetrators in past cases of oil cargo thefts and risk assessment, the following are recommended measures to be taken by the ship manager, ship master/crew before the voyage.

#### Ship Manager / CSO

- Must be updated of the latest situation through reports promulgated by the ReCAAP ISC and IFC, and brief crew during planning and before sailing while advising the master and crew to exercise vigilance especially when transiting vulnerable areas.
- Establish an effective ship's security and communication plan including a back-up plan in case the primary mode of communication failed and ensure that the crew know about these plans.
- Compartmentalize information on a "need-to-know" basis, particularly the type and volume of the cargo oil the ship is carrying to ensure the confidentiality of the information.
- Conduct regular background checks of crew to ensure their credibility and aware of the crew's activities on board the ship and while ashore.
- Ensure that the master and crew know the importance of timely reporting to flag State and coastal State in accordance with Maritime Safety Committee Circular 1334; and have readily compiled contact details before start of voyage.
- Establish SPMs, for instance rigging up physical barriers and installing security equipment on board ship such as alarms, CCTVs, tracking devices and others to detect and deter perpetrators from boarding the ship.
- Ensure that the ship security officer has conducted random inspection and checks on the ship, crew and cargo before set sail.

## Ship Master / Crew

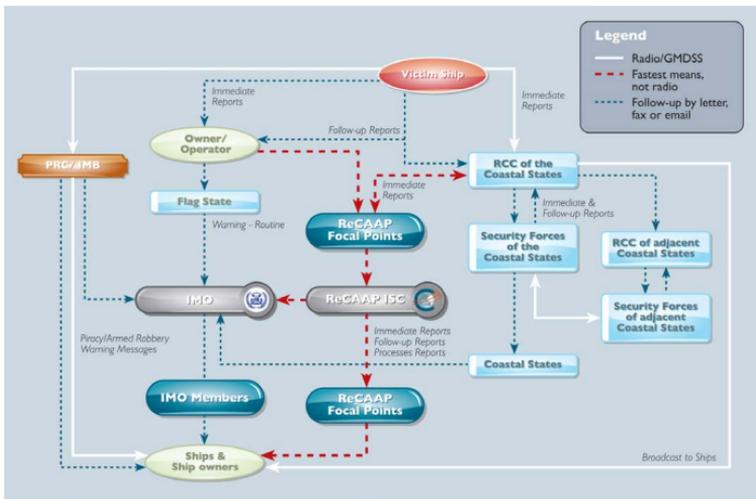
- Adopt best practices in anti-piracy efforts and other relevant elements of BMP 4.
- Equip with an updated list of authorities of the coastal States to contact in case of any eventualities.
- Inform enforcement agency in the nearest coastal State of the ship's planned movement, especially when transiting areas that were vulnerable.

### 3.7 Reporting

Ship owner/CSO/master/crew may refer to the following recommended charts and reporting channels for pre-voyage planning, during voyage and in the event of piracy or sea robbery attack. Following any attack or suspicious activity, ship master is encouraged to make a detailed report of the incident to the authorities and the shipping company. The proposed format of reporting of an incident can be found in Annex B.

#### (A) IMO's Maritime Safety Committee Circular (MSC) Circular 1334

To seek immediate response from the enforcement agencies at sea, ship master should report to the Rescue Coordination Centre (RCC) of the coastal State, and ship owner/operator upon notified by the master to report to the flag State and ReCAAP Focal Point; as in accordance with the IMO MSC.1/Circ 1334 on *Guidance to ship owner, ship operator, ship master and crew on preventing and suppressing acts of piracy and armed robbery against ships*. The flow diagram of the IMO MSC Circular 1334 for reporting of incidents in Asia is as shown.



Flow Diagram for Reporting Incidents in Asia

## **(B) Maritime Security Planning Charts**

The Maritime Security Planning Charts, Q6112 (Karachi to Hong Kong) and Q6113 (Andaman Islands to Torres Strait) issued by the United Kingdom Hydrographic Office (UKHO) supported by the ReCAAP ISC and IFC are for shipping companies to plan their route; and provide situation awareness for masters when their vessels transiting the area. In conjunction with IMO MSC.1/Circ 1334, the charts contain the contact details of ReCAAP Focal Points. The IFC has also features their Voluntary Community Reporting features in the charts. Launched on 17 May 2013, the purpose of the charts is to cover existing maritime security threats of which piracy is one of them, and to enable quick promulgation of future threats to mariners.

## **(C) ReCAAP Focal Points Reporting**

In accordance with the IMO MSC.1/Circ 1334, ships owners/operators are to report all incidents in Asia to the ReCAAP Focal Points. As the RCCs of some ReCAAP Contracting Parties are also ReCAAP Focal Points; Focal Points upon receipt of information from the ship owners/operators will also disseminate the information internally to their respective RCCs, maritime authorities and enforcement agencies as appropriate. Multi-sources of information gathered by the Focal Points enable the relevant authorities to respond to an incident promptly in accordance with their national policies and jurisdiction. The contact details of the ReCAAP Focal Points and Contact Point can be found in Annex C.

## **(D) Voluntary Community Reporting**

Vessels are encouraged to participate in the voluntary community reporting program administered by the Information Fusion Centre (IFC). The IFC encourages ships in the IFC Area of Interest (AOI) to report to IFC using the reporting format described in the Voluntary Community Reporting (VCR) scheme when entering the IFC's AOI. Please refer to Annex D.

## SECTION 4

# MARITIME SECURITY PLANNING CONSIDERATIONS

### 4.1. Pre-sailing

#### Checklist for Ship manager / CSO

Establish and update the Ship Security Plan (SSP).

Establish a distress codeword which is only known between the owner/CSO and master.

Establish and update the Ship Emergency Communication Plan (SECP).

Establish and conduct regular communications check (primary and back-up net) with master.

Update the list of contact details for incident reporting.

Emphasize the importance of timely reporting of incident to the coastal State.

Establish reporting procedures (both routine and emergency).

Obtain the latest situation update from the ReCAAP ISC and IFC websites for updates/situational awareness on piracy and armed robbery against ships and brief the master/crew.

Conduct of background checks on crew.

Ensure non-homogeneous crew, if possible.

Conduct checks on logistics manifest (e.g. quantity of oil cargo, cans of paint) to ensure items brought are not in excessive amount.

Inform nearest coastal State of ship's planned route.

Conduct risk assessment of planned route and review if necessary.

Ensure adequate manpower on board ships for watch-keeping duties.

Install relevant ship physical protection measures on board (e.g. lightings, tracking devices, CCTV), if possible.

Educate the crew about evidences management (gathering and preservation) in the event of piracy/sea robbery incident.

## Checklist for **Ship master / crew**

Familiarise with the SSP and ISPS code requirements.

Familiarise with the SECP.

Assign specific task, responsibilities and role for each individual (during routine or time of emergency).

Conduct inventory check of ship's communication equipment.

Familiarise with ship's physical protection measures and security equipment on board (e.g. alarms and lighting system).

Ensure that possible avenues of boarding are well illuminated.

Conduct drill on emergency reporting / communication procedures.

Conduct anti-piracy drill.

Conduct risk assessment.

## 4.2. During sailing

### Checklist for **Ship manager / CSO**

Establish routine and periodical communication with the ship in accordance with its SSP and SECP.

Continuously monitor the ship's position, speed and movement.

Request master to provide a SITREP at regular intervals.

Maintain situational awareness/monitor updates on incidents of piracy and sea robbery from ReCAAP ISC and IFC websites.

### Checklist for **Ship master / crew**

Update shipping company on the position and movement of ship at regular intervals and shorten reporting period especially transiting in vulnerable areas.

Submit SITREP to the CSO at regular intervals.

Establish systematic and continuous communication with shipping company and crew on board.

Prepare an emergency communication plan to include all essential emergency contact numbers and pre-prepared messages.

Avoid, whenever possible, coastal navigating in vulnerable areas.

Maintain all-round vigilance and lookouts. Security monitoring equipment on board is to be utilised whenever necessary.

Ensure radars are properly manned and operated to keep a lookout for approaching and suspicious-looking vessels.

Brief crew on the preparation and their respective duties prior entry into vulnerable areas.

Minimize all maintenance and engineering work; and work outside the accommodation quarters in vulnerable areas.

Control all possible access / entry points while transiting vulnerable areas.

Ensure all engine room essential equipment (e.g. water/fire pumps) is in ready-condition when sailing in vulnerable areas.

Exercise crew with ship security systems and ship security contingency plans to ensure a clear understanding and expectation of actions should the ship be boarded by pirates or armed robbers.

## SECTION 5

# SHIP PROTECTION MEASURES

The following are SPMs recommended for adoption by shipping companies for their ships when underway in vulnerable areas:

### 5.1. Recommended physical measures

- To discourage and deter boarding and access to the ship's accommodation, ship should consider implementing strong hardening measures such as barbed/razor wire barriers, spikes or other industry recognised methods as deemed appropriate.
- All doors and hatches, not just those facing the weather deck, but including interior ones providing access to the bridge, accommodation and machinery spaces must be properly secured to prevent them from being opened.
- Hatches can be reinforced with measures such as Padlock/Angle Bar Protection Box which reinforce weather-tight doors by preventing easy cutting or knocking of padlocks and eye-pads. However, such measures will be useless if poor quality padlocks are used. A regular review on padlock quality for suitable size, its security grades [EN12320] and water-proofing is necessary.



- In addition to the padlocking of the skyline hatch from outside, sling wire-lashing from the inside of the ship's stores onto the hatch can be made with the end secured to a turn-buckle to prevent slack. Without a turn-buckle, the hatch can still be breached and the sling wire-lashing may slack through vibration or other factors.



- A designated and limited number of access points must be used for security patrols and routine access. The use of these doors or hatches must be controlled by the Officer of the Watch.
- Means of blocking or lifting external ladders on the accommodation block to prevent use and to restrict external access to the bridge.
- Barbed/razor wire barriers can be emplaced in particularly vulnerable, lower-entry zones of the ship, such as the low freeboard areas. In case of time restrictions, these areas ought to be hardened first whereas the remaining areas do so while the ship is underway. Due consideration to be accorded for crew evacuation should the need arises.



- Accommodation port holes and windows which could be used to gain access to the ship accommodation must be fitted with hardening arrangements such as dead lights or interior grilles. To facilitate evacuation in times of safety hazards, mechanisms such as variable bolts and butterfly latches can be used to secure the interior grilles:



- Water sprays should be rigged - hoses and foam monitors (delivering water) in a ready state should be fixed in position to cover likely access routes, particularly the vulnerable quarter decks and other blind spots on board the ship:



- Tools and equipment that may be of use to attackers must be stored in a secure location



- Alarms – the alarm systems are important and useful to warn the crew on board regarding threat or intrusion. Alarm likewise serves as an alert to the perpetrators that they had been detected, thus, it has been an effective tool in compelling the perpetrators to leave after knowing that they had been spotted.



- Ship Security Alert System (SSAS) – In compliance with ISPS Code and guidelines from IMO, operational status of the SSAS should be checked prior each voyage and the familiarization of crew should be carried out with its functionality and discreet operations periodically.



- Tracking devices and communications equipment enable marine and naval ships to track, identify and monitor a ship's position, location and any other detail that might be important in manoeuvring and stabilizing a ship's route and course. The use and installation of different types of tracking devices and communication equipment gives added advantage to the ships especially during times of distress.
- Emergency communications equipment, such as iridium-powered phones, can be stowed on board and used in case of the ship's main communications were disabled by perpetrators. A backup iridium-powered phone should also be stowed in a secure location or any safe room.



- Search Light/Lighting – the use of search lights is useful as it can detect any approaching ships or boats at greater distance and can be used as a signalling device. Having sufficient lighting around the ship is also a source of deterrence to pirates and robbers at night whether the ship is at port or underway. Lighting can provide maximum illumination within and around the decks giving the watches and lookouts better view around the ship.



- Close-circuit television (CCTV) – is useful to ensure that vulnerable locations of ship are monitored, and the owner is able to view these vulnerable portions in the owner's control room ashore and on board the ship manned by an operator.
- It is advisable to install a CCTV outside the master's cabin for the ship master to monitor exterior situations.



## 5.2. Additional measures

The following additional measures can be considered by ship managers or CSOs:

- Fabricated steel plating on the weather deck doors for protection against firearms.
- Polycarbonate screens that are lightweight and damage-resistant for additional protection of the bridge area.
- Motion sensors (infra-red or laser) especially in vulnerable areas such as the quarter decks and entrances to detect suspicious movements.
- Commercial software that allows the ship manager or CSO to remotely monitor any attempts of oil cargo theft or disabling of AIS on board the ship.
- Commercial software to allow the ship manager or CSO onshore to track the ship on voyage.
- Citadel – with bulletproof doors, emergency rations lasting at least 72 hours, as well as USB plug for crew to remotely monitor the exterior via CCTV. The crew should be aware of the procedures of evacuation to the citadel and exercise regularly on swift evacuation in case of inevitable boarding by the perpetrators. The citadel which provides protection must ensure a reliable means of communication ashore to maintain certain degree of situation awareness and responses from the authorities. As it provides resistance to forced entry for a fixed period of time, due consideration is necessary to ensure the ability to control the ship to avoid collision especially in busy waters.

## SECTION 6

# SHIPS UNDER ATTACK

### Checklist for **Ship manager / CSO**

Report incident to the flag State, relevant authorities and ReCAAP Focal Points (see Annex C on contact details).

Provide details of the incident based on the specified format in this guide.

Maintain continuous contact with ship master and crew.

Monitor the ship's position, speed and direction closely.

Inform local shipping organisations of the incident.

Direct/remind ship master/crew to execute SSP/SECP.

### Checklist for **Ship master / crew**

Report incident immediately to the nearest coastal State, ship owner, authorities and ships within the vicinity (see MSC Circular 1333/1334).

Sound the emergency alarm.

Activate security alert systems.

Muster all crew and inform them about the situation.

Block all possible access and entry points.

Activate physical security protection measures on board, if any.

Remain in continuous contact with ship owner and authorities.

Do not resist the perpetrator should they manage to board the ships.

Remain calm.

Observe details of the perpetrators (e.g. physical and facial features, attire, language, nationality, type of weapons used, boats used for boarding, direction of escape route perpetrators took).

Keep the CCTVs on.

Switch on the emergency lighting system during hours of darkness.

Assess the situation.

Proceed to nearest port and inform the maritime/port authorities (if possible).

## SECTION 7

# ROLE OF MARINER IN IMPROVING SITUATION IN THE REGION

With the increase in oil cargo thefts in the Asian region during the period of 2011 till September 2015, shipping companies are facing the challenges of ensuring the safety of not just the oil cargoes on board their ships but most importantly, the safety of their crew.

Therefore, it is important for ship managers and masters to be cognisant of the latest situation and locations where relatively high number of incidents had been reported. Having such knowledge furnishes the option of avoiding routes through vulnerable areas. If it is not possible to avoid these routes, such knowledge will also promote higher level of vigilance during transit through these areas.

Based on joint studies performed by the ReCAAP ISC and its operational partners, the timing of boarding by perpetrators and the appearance of another tanker/barge to come alongside the victim ship appears to be more than coincidence. In most of the incidents, the perpetrators seemed to possess knowledge of the oil cargo carried on board the ship, its route and schedule.

As such, it is important for shipping companies to ensure the confidentiality of the type of oil cargo as well as the ship's intended route and schedule. Risk assessments in the following basic aspects ought to be conducted prior to the voyage.

### 7.1. Condition of the ship, crew and cargo

#### Ship

- Must be compliant with ISPS code requirements.
- Must be first and foremost seaworthy, taking into consideration its class certification, stability, equipment, operational limitations (speed, manoeuvrability, and freeboard) and restrictions.
- Must carry corresponding Maritime Security Planning Chart and navigation charts and other navigational equipment.
- Must be equipped with hardened measures/physical measures to ensure deterrence or denial against any possible boarding and attack.

#### Crew

- Crew must be competent, well-trained in anti-piracy measures and sufficient in number.
- Crew must be certified and had their backgrounds properly screened.

## Cargo

- Cargo must be laden and stowed safely and securely.

## 7.2. Route or intended course of the vessel

### Voyage Plan

- Must be prepared to include a review of all information relative to the voyage, taking into account the condition of the vessel, characteristics of the oil cargo, provision of competent crew, charts, guides and navigational equipment.
- Must cover the entire voyage from port to port, including direction and procedures to report to proper authorities in the area of operation where piracy or armed robbery was known to occur.

### Security Plan

- Must include crisis management plan for the purpose of responding to incidents as well as contingency arrangements to cope with boarding, and reporting, providing evidence as needed by authorities to prosecute perpetrators, and returning to normal condition as soon as possible.
- Must increase the frequency of periodical reporting to shipping companies, managers or CSOs or regional centres, especially when transiting through vulnerable areas.

## 7.3 Situational awareness

### Location

- Masters and Ship Officers must be aware of areas of relatively high number of incidents and decide on alternative routes which can be undertaken whenever the situation arises.
- Crew must be aware of the conditions for the transit area (calm/rough sea condition and visibility), especially the time (day/night) when the ship transits any area of higher than normal risk.

### Advisories/Reports

- Shipping companies/CSOs are to be apprised of reports produced by the ReCAAP ISC and IFC on piracy and sea robbery which provide analysis regarding the general situation in regional waters, in particular areas of concern.

### Coordination

- The shipping company or ship must coordinate with and inform the relevant enforcement agencies in the area of the planned voyage, especially if the route is considered vulnerable to boarding or has had previous occurrences of boarding.
- Frequent communication checks with the ship company's shore management teams to ascertain normalcy of passage and report concerns when they arise.

## SECTION 8

# POST-INCIDENT REPORTING AND FOLLOW-UP

### Checklist for **Ship manager / CSO**

Cooperate with authorities and provide updates.

Provide essential information, documents and identification of crew and vessel.

Cooperate with authorities during the conduct of investigation.

Ensure crew are readily available during conduct of investigation.

Provide follow-up reports and gather feedback on investigation outcome.

Provide assistance to crew and their families.

Share experience and lessons learned during conferences, forums, meetings etc.

Develop and share Best Management Practices.

Submit Post Incident Report as per IMO circular 1334 [see Section 3.7 (a)].

### Checklist for **Ship master / crew**

Provide details of the incident and updates to ship owner/company.

Provide additional details and information to authorities.

Preserve/document (e.g. back up a copy of the CCTV footage during the incident, if possible) but do not tamper with all available evidences on board the ship. Refer to IMO reference A28/Res. 1091 dated 28 March 2014 on the *Guidelines on Preservation and Collection of Evidence Following an Allegation of a Serious Crime Having Taken Place on board a Ship or Following a Report of a Missing Person from a Ship, and Pastoral and Medical Care of Persons Affected*.

Share information and experience with investigators/seafarers.

## ANNEX A

# DEFINITIONS

**Piracy**, in accordance with Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS), is defined as:

1. "Piracy" means any of the following acts:
  - (A) 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:
    - (i) on the high seas, against another ship, or against persons or property on board such ship;
    - (ii) against a ship, persons or property in a place outside the jurisdiction of any State;
  - (B) 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;
  - (C) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

**Armed Robbery Against Ships**, in accordance with the Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships of the International Maritime Organisation (IMO) Assembly Resolution A.1025(26), is defined as:

2. "Armed robbery against ships" means any of the following acts:
  - (A) any illegal act of violence or detention, or any act of depredation, or threat thereof, other than an act of "piracy", committed for private ends and directed against a ship, or against persons or property on board such ship, within a State's internal waters, archipelagic waters and territorial sea;
  - (B) any act of inciting or of intentionally facilitating an act described above.

# ANNEX B

## REPORTING FORMAT

---

### Reporting Format (as per MSC.1/Circ 1334)

- Ship's name and IMO number
- Type of ship
- Flag
- Gross tonnage
- Date and time
- Latitude and Longitude
- Name of the area
- While sailing, at anchor or at berth
- Method of attack
- Description/number of suspect craft
- Number and brief description of pirates/robbers
- What kind of weapons did the pirates/robbers carry?
- Any other information (e.g., language spoken)
- Injuries to crew and passengers
- Damage to ship (Which part of the ship was attacked?)
- Brief details of stolen property/cargo
- Action taken by the master and crew
- Was incident reported to the coastal authority and to whom?
- Reporting State or international organization
- Action taken by the coastal State

# ANNEX C

## CONTACT DETAILS

### Contact Details of ReCAAP Focal Points and Contact Point\*, ReCAAP ISC, IFC, and Malaysian Authorities

(\* Please refer to the ReCAAP ISC Mobile App for the updated contact details of the ReCAAP Focal Points and Contact Point.)

ReCAAP FOCAL POINTS / CONTACT POINT		
Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
<b>Australia</b>		
Australian Maritime Border Operations Centre (AMBOC) Maritime Border Command (MBC) E-mail: amboc@border.gov.au	+61-2-6275-6000	+61-2-6275-6275
<b>Bangladesh</b>		
Department of Shipping E-mail: cns@dos.gov.bd	+88-02-9553584	+88-02-9587301
<b>Brunei</b>		
National Maritime Coordination Centre Brunei Email: p2mk@jpm.gov.bn	+673-2233751	+673-2233753
<b>Cambodia</b>		
Merchant Marine Department E-mail: mmd@online.com.kh	+85-5-2386-4110	+85-5-2386-4110
<b>China</b>		
China Maritime Search and Rescue Centre (Beijing) Email: cnmrcc@mot.gov.cn	+86-10-6529-2218 +86-10-6529-2219 +86-10-6529-2221	+86-10-6529-2245
Maritime Rescue Coordination Centre (Hong Kong) Email: hkmrcc@mardep.gov.hk	+85-2-2233-7999 +85-2-2233-7998	+85-2-2541-7714

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
<b>Denmark</b>		
Danish Maritime Authority (DMA) Email: ReCAAP-FP-DK@dma.dk	+45-9137-6000	+45-9137-6001
<b>India</b>		
MRCC (Mumbai) Coast Guard Region (West) Mumbai – India Email: indsar@vsnl.net icgmrc_mumbai@mtnl.net.in mrcc-west@indiancoastguard.nic.in	+91-22-2431-6558 +91-22-2438-8065	+91-22-2433-3727 +91-22-2431-6558
<b>Japan</b>		
Japan Coast Guard (JCG) Ops Centre Email : jcg-op@milit.go.jp	+81-3-3591-9812 +81-3-3591-6361	+81-3-3581-2853
<b>Republic of Korea</b>		
Ministry of Oceans and Fisheries Operations Centre Email: piracy@gjcoms.go.kr	+82-44-200-5895 to 98	+82-44-200-5886 to 88
<b>Laos</b>		
International Relation Department Ministry of Public Security Email: keo_kkk@hotmail.com	+85-6-2121-2505	+85-6-2121-2505 +85-6-2121-2547
<b>Myanmar</b>		
MRCC Ayeyarwaddy (Myanmar Navy) Email: mrcc.yangon@mpmail.com.mm	+95-313-1650	+95-1202-417
<b>Netherlands</b>		
Dutch Coastguard Maritime Information Centre (MIK-NL) Email: mik-nl@kustwacht.nl	+31-223-658-382	+31-223-658-358
<b>Norway</b>		
Norwegian Maritime Authority Email: morten.alsaker.lossius@sjofartsdir.no	+47-5274-5000 +47-5274-5130	+47-5274-5001

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
<b>Philippines</b>		
Philippine Coast Guard PCG Action Centre-MRCC (Manila) Email: pcg_cg2@yahoo.com cg2@coastguard.gov.ph isc.cg2@coastguard.gov.ph	+63-2-527-3877 +63-2-527-8481 to 89 (ext: 6136/6137) +63-917-724-3682 (Text Hotline) +63-2-527-8481 loc6122	+63-2-527-3877
<b>Singapore</b>		
Maritime and Port Authority of Singapore Port Operations Control Centre (POCC) Email: pocc@mpa.gov.sg	+65-6226-5539 65-6325-2493	+65-6227-9971 +65-6224-5776
<b>Sri Lanka</b>		
Sri Lanka Navy Operations Centre Email: nhqsoo@navy.lk nhqhydrographer@navy.lk nhqdn@navy.lk	+94-11-244 5368	+94-11-244 9718
<b>Thailand</b>		
Royal Thai Navy Maritime Information Sharing Centre (MISC) Email: miscdutyofficer@misc.go.th	+66-2475-4532	+66-2475-4577
<b>United Kingdom</b>		
National Maritime Information Centre Operations Centre Email : nmic-ws@mod.uk	+44 2392-211951	+44 2392-212024 Please indicate "FAO NMIC – A leg" if send via fax
<b>United States</b>		
USCG Rescue Coordination Center Alameda (RCCAlameda) Email: rccalameda@uscg.mil	+1-510-437-3701	

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
<b>Vietnam</b>		
Vietnam Coast Guard Email : vietnamcoastguard@gmail.com vietnamfocalpoint@yahoo.com.vn	+84-4-3355-4378	+84-4-3355-4363

Correct as at 12 October 2015

<b>AGENCIES</b>		
ReCAAP Information Sharing Centre (ISC) Email: info@recaap.org	+65-6376-3091	+ 65-6376-3066
Information Fusion Centre (IFC) Email : ifc_dof@defence.gov.sg	65-6594-5728 (During office hours) +65-9626-8965 (After office hours)a	+65-6594-5734
Malaysian Maritime Enforcement Agency (MMEA)		
Northern Region	604-9669800	604-9660542
Southern Region	607-2199400	607-2236101
Eastern Region	609-5717300	609-5733569
Sabah Region	608-838 5000 608-8524600	608-838 4161
Sarawak Region	608-2432553 608-2432544	608-2432502

## ANNEX D

# VOLUNTARY COMMUNITY REPORTING

The VCR merchant vessel voluntary reporting schemes has been established by the IFC for the purpose of enhancing security and provide the necessary support to maintain the freedom of navigation of all vessels in Southeast Asia and surrounding waters.

Merchant vessels operating in the VCR region are strongly encouraged to report maritime security incidents or anomalous behaviour to the IFC. Any vessel, owner, operator or manager choosing not to report may delay any assistance in the event of an incident as military and maritime enforcement assets will not be expecting the ship, resulting in valuable information not being available.

The Owners/Masters of the vessels are encouraged to send regular reports of their position/course/speed and other voyage information as well as report on anomalous activities to the IFC. In return, IFC provides maritime security advisories to the ships based on their reported position and intended destinations. IFC will risk evaluate and monitor selected vessels, sharing the information with other maritime enforcement agencies when required. Ships are encouraged to report under the following conditions:

- A) When transiting in Southeast Asia.
- B) Any items changed from the initial report.
- C) On the occurrence of a maritime security incident.
- D) Observing any suspicious or anomalous behaviour.

Participation in this reporting scheme is totally free and vessels sailing under any flag are strongly encouraged to participate. All information provided is treated with strict commercial confidentiality and will be used within the military and maritime enforcement agencies.

Anomalies are behaviours outside the normal expectations of shipping, commercial trade, or marine practice. They may be indicative of a maritime security threat. These can include, but are not limited to, the following:

- Unusual RVs of ships at sea including transfers of cargo or people
- Darkened ships/not illuminating nav lights
- Ships anchored in unusual locations
- Ships not flying a flag/displaying a name

- Ships navigating contrary to the ordinary practice of seamen
- Vessels outside of normal patterns/sea lanes
- Fishing boat without appropriate equipment
- Overcrowded/unseaworthy/overloaded vessels
- Non-ocean going vessels in the high seas
- Abandoned vessels
- Unwarranted/unsolicited approaches by vessels to your own vessel or other vessels in your vicinity
- Non-military/government vessels carrying arms
- Vessels carrying boarding equipment
- Suspicious/unusual voice communications
- Vessels underway/making way without AIS transmission

It is recommended that the VCR reports consist of the following fields of information and be sent to [information\\_fusion\\_centre@defence.gov.sg](mailto:information_fusion_centre@defence.gov.sg)

Initial Report	
01	Ship Name
02	Flag
03	IMO Number
04	Inmarsat Telephone Number
05	Time & Position
06	Course
07	Passage Speed
08	Freeboard
09	Cargo
10	Destination and Estimated Time of Arrival
11	Name and Contact of Company Security Officer
12	Nationality of Master and Crew
13	Armed/Unarmed Security Team Embarked
14	Company (Contact Details and Email)

Daily Position Report	
01	Ship Name
02	International Radio Call Sign (IRCS)
03	IMO Number
04	Time of Report (UTC)
05	Ship Position
06	Course / Speed
07	Any Other Important Information
08	Company

Final Report	
01	Ship Name
02	International Radio Call Sign (IRCS)
03	IMO Number
04	Time of Report (UTC)
05	Port or Position
06	Company

Suspicious Activity Report	
01	Ship Name
02	IMO Number
03	Type of suspicious activity
04	Position of incident
05	Details of incident
06	Inmarsat number
07	Email address to be contacted by
08	Date and Time of report (at GMT)
09	Company

# IFC Voluntary Reporting Area



## ANNEX E

# PARTNER ORGANISATIONS

### IFC

The Information Fusion Centre or IFC is a 24/7 regional Maritime Security (MARSEC) information-sharing centre. It was inaugurated on 27 Apr 2009 and aims to facilitate information-sharing and collaboration between partners to enhance maritime security. Through the speedy sharing of information, we facilitate timely responses with our partner countries on maritime incidents. We also aim to achieve early warning of maritime security threats by building a common maritime situation picture and acting as a maritime information hub for the region.

The IFC is manned by an integrated team of International Liaison Officers (ILO) from various navies/coastguards, and RSN personnel. We have wide and extensive linkages with more than 65 agencies in 35 countries. The ILOs serve as the conduit to their respective countries' various agencies' operation centres in facilitating the seamless sharing of information between their parent agencies and the IFC.

The IFC works with the shipping community to enhance maritime security through regular activities such as the Shared Awareness Meeting (SAM) and Tiger Team Visits (TTV) to companies. The Voluntary Community Reporting (VCR) is one of the initiatives by IFC to engage the shipping community through information sharing and reporting. In return, IFC shares shipping advisories to the VCR members through its weekly reports, monthly maps and SMS alerts warning mariners about the situation at sea. The IFC also conducts capacity-building activities on international information-sharing exercises and MARSEC workshops such as the biennial Maritime Information Sharing Exercise (MARISX) and the annual Regional Maritime Security Practitioner Course (RMPC). The IFC also hosts maritime information sharing portals such as the ASEAN Information Sharing Portal and the Regional Maritime Information exchange (ReMIX), which facilitates information sharing among ASEAN navies and Western Pacific Naval Symposium members.

### ReCAAP ISC

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is the first regional government-to-government agreement to promote and enhance cooperation against piracy and armed robbery in Asia. It was finalized on 11 November 2004 and entered into force on 4 September 2006. To date, 20 States have become Contracting Parties to ReCAAP.

The 20 Contracting Parties to ReCAAP are Australia, the People's Republic of Bangladesh, Brunei Darussalam, the Kingdom of Cambodia, the People's Republic of China, the Kingdom of Denmark, the Republic of India, Japan, the Republic of Korea, the Lao People's Democratic Republic, the Republic of the Union of Myanmar, the Kingdom of the Netherlands, the Kingdom of Norway, the Republic of the Philippines, the Republic of Singapore, the Democratic Socialist Republic of Sri Lanka, the Kingdom of Thailand, the United Kingdom, the United States of America and the Socialist Republic of Viet Nam.

The ReCAAP Information Sharing Centre (ReCAAP ISC) was established under the Agreement, and was officially launched in Singapore on 29 November 2006. The roles of the ReCAAP ISC are to:

- serve as a platform for information exchange with the ReCAAP Focal Points via the Information Network System (IFN); facilitate communications and information exchange among participating governments to improve incident response by member countries; analyse and provide accurate statistics of the piracy and armed robbery incidents to foster better understanding of the situation in Asia;
- facilitate capacity building efforts that help improve the capability of member countries in combating piracy and armed robbery in the region; and
- cooperate with organizations and like-minded parties on joint exercises, information sharing, capacity building programme, or other forms of cooperation, as appropriate, and agreed upon among the Contracting Parties.

The ReCAAP ISC facilitates exchange of information among the ReCAAP Focal Points through a secure web-based Information Network System (IFN). Through this network, the ReCAAP Focal Points are linked to each other as well as the ReCAAP ISC on a 24/7 basis, and are able to facilitate appropriate responses to incident. The agency receiving the incident report will manage the incident in accordance with its national policies and response procedures, and provide assistance to the victim ship where possible. The agency will in turn, inform their ReCAAP Focal Point which will submit an incident report to the ReCAAP ISC and its neighbouring Focal Points. For more information about the ReCAAP and ReCAAP ISC, please visit <http://www.recaap.org>.

## RSIS

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous school within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education with a strong practical emphasis
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy
- Foster a global network of like-minded professional schools

### Graduate Education in International Affairs

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (MSc) degree programmes in Strategic Studies, International Relations, Asian Studies, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from more than 50 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS.

A small but select PhD programme caters to advanced students who are supervised by faculty members with matching interests.

### Research

Research takes place within RSIS' five components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National Security (CENS, 2006), the Centre for Non-Traditional Security Studies (Centre for NTS Studies, 2008); and the Centre for Multilateralism Studies (CMS, 2011). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

The school has five endowed professorships that bring distinguished scholars and practitioners to teach and to conduct research at the school. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, the NTUC Professorship in International Economic Relations, the Bakrie Professorship in Southeast Asia Policy, and the Peter Lim Professorship in Peace Studies.

## **International Collaboration**

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as learn from the best practices of successful schools.











**Regional Cooperation Agreement**  
**on Combating Piracy and Armed Robbery against Ships in Asia**  
21 Media Circle, #05-04, Singapore 138562  
**T** +65 6376 3091 | **F** +65 6376 3066 | **E** info@recaap.org | **W** www.recaap.org