Maritime security instruments in practice: a critical review of the implementation of ISPS code in the port of Hong Kong

Koi Yu Adolf Ng

Department of Logistics and Maritime Studies, The Hong Kong Polytechnic University, Hong Kong.
Tel: (852) 3400 3625
Fax: (852) 2330 2704
Email: lgtan@polyu.edu.hk

Abstract

The 9/11 terrorist attack has exposed the brittleness of the transportation system which can lead to unprecedented disruption of the global trade system. In responding to such challenge, various security enhancement instruments have been introduced by the international community, notably the ISPS Code. Although various works on maritime security had been undertaken, works dedicated to port security outside developed, western economies, like Asia, remained very scarce, where comprehensive review on how such international guidelines can be applied in a local perspective was found wanting. Hence, focusing the port of Hong Kong, this paper critically reviews how the ISPS Code has been promulgated and implemented in a local perspective. This paper argues that the port of Hong Kong is largely a follower rather than an innovator in complying with the ISPS Code and that port security is perceived as more a problem to solve rather than an opportunity to innovate. This paper can provide valuable insight on the problems, obstacles and solutions when promulgating and implementing maritime security instruments to different global regions.

Keywords: maritime, port security, ISPS Code, Hong Kong

1. Introduction

The outbreak of 9/11 terrorist attack has exposed the potential brittleness of the transportation system. A terrorist event involving the system could lead to unprecedented disruption of the global trade system (Flynn, 2006) which would not only involve human casualties, but also economic, political and social impacts, notably the breakdown of global supply chains and potentially global economic recessions (Greenberg et al., 2006), and it becomes clear that further and, perhaps radical, changes are needed to maximize maritime and supply chain securities in the 21st century (Mensah, 2003).

Being nodal points, port security is arguably pivotal in ensuring the smoothness and efficiency of an increasingly complex intermodal logistical supply chains (Robinson, 2002; Ng, 2007). As defined by Ng and Gujar (2008), port security includes all security and counterterrorism activities which fall within the port domain, including the protection of port facilities, as well as the protection and coordination of security activities when ship and port interact[1]. Although a number of works on maritime security had been undertaken, both academic (for instance, see: Mensah, 2003; Bichou, 2004; King, 2005; Zhu, 2006; Bichou et al., 2007; Talley, 2008) and industrial (for instance, see: OECD, 2003; Greenberg et al., 2006), works dedicated to port security had, so far, remained scarce, or rather being technical in nature (for instance, see: Bichou, 2004; Kumar and Vellenga, 2004), where comprehensive review on how such maritime security instruments can be applied in a local perspective, including obstacles and solutions, is clearly lacking. Even within these few works, attention has often focused on developed, western economies (for instance, see: Ng, 2007; Pallis and Vaggelas; 2007 and 2008; Pinto et al., 2008) where comprehensive analysis on other regions,

[1] Despite the broad definition of port security, since 9/11, much attention had been paid on fighting the threats from terrorist attacks, of which this is also the focus of this paper.

including various globally important economic regions in Asia, remains largely unjustifiably understudied, or simply descriptive rather than analytical in nature (for instance, see: Huxley, 2005; Tan, 2005), possibly with the works of Ng and Gujar (2008) being the only notable exception, thus leaving significant research gaps yet to be filled.

To address such deficiency, through investigating the port of Hong Kong, this paper provides a critical analysis on how the international requirements on port security, as decided by the International Maritime Organisation (IMO), have been imposed in a local perspective. The remaining of this paper is as follows. Sections 2 and 3 will briefly discuss the major international mechanisms initiated by International Maritime Organisation (IMO) related to port security, i.e., the ISPS Code, as well as the research methodology. After then, section 4 will discuss how such guidelines have been implemented in the port of Hong Kong. Before the conclusion in section 6, section 5 will discuss the major challenges that ports are currently facing in addressing port security issues, and how they should improve this situation.

2. The ISPS Code and Port Security

At international level, port security is governed by rules issued by IMO based on the amendments made in December 2002 to the *International Convention for the Safety of Life at Sea* (SOLAS) 1974 as amended, as well as the addition of *Special Measures in Enhancing Maritime Security* (Chapter XI-2) to SOLAS, resulting in the introduction of the *International Ship and Port Facility Security (ISPS) Code*, adopted by IMO on December 2002 and fully implemented on 1 July 2004[2] [3]. Being labelled as the 'comprehensive security regime for international shipping' (Mensah, 2003), deliberate guidance on maritime security, including ports, has been included in the ISPS Code. It is important to note that, however, the code primarily addresses how terrorist attacks can be deterred and minimized, whereas the detailed procedures in addressing the aftermath of a significant security incident, i.e. crisis management, are not mentioned. Indeed, by the time when this paper is written, significant security incidents in ports have yet to take place.

In compliance with the ISPS Code, all ships over 500 gt and port facilities are required to conduct vulnerability assessments and develop security plans to deter potential terrorist attacks e.g. passenger, vehicle and baggage screening procedures, security patrol, the establishment of restricted areas and its execution, procedures for personnel identification, access control, installation of surveillance equipment, etc. The main objectives of the ISPS Code include: (i) detecting security threats; (ii) implementing security measures; (iii) collating and promulgating information related to maritime security; (iv) providing a reliable methodology in assessing maritime security risks; (v) developing detailed security plans and procedures in reacting to changing security levels; and (vi) establishing security-related roles and responsibilities for contracting governments (and their administrations), ship companies and port operators at national and international levels, including the provision of

[2] Despite the international nature of the ISPS Code, however, it was very much an American initiative led by the US Coast Guard, being part of the US government's response to the tragic events of 9/11 with the target of creating a consistent security programme for ships and ports (and their operators and governments) to identify and deter threats from terrorists more effectively.

[3] Apart from international initiatives as mentioned above a number of US-initiated programmes had also been promulgated, many of which have de facto become global port security programmes due to the US's global influences, notably the Container Security Initiative (CSI) and the Custom-Trade Partnership Against Terrorism (C-TPAT), which have been formally codified into law in the US through the Security and Accountability for Every Port Act (SAFE Port Act), adopted in 2006. Apart from the codification of law, the SAFE Port Act also provides further guidance in enhancing port security which is perceived to pose significant global implications, e.g. additional requirements for maritime facilities, transport worker identification credential, port security grants, foreign port assessments, establishment of interagency operational centres for port security, etc. SAFE Port Act was adopted largely in response to the political chaos due to the sale of P&O Ports, including its US port assets, to Dubai Ports World (DPW). The ensuing controversy had led to charges that such purchase could pose a significant national threat. Facing such dilemma, in December 2006, DPW sold its US port assets to AIG. Given the paper's objective, however, this section only reviews the ISPS Code and its impacts on port security.

professional training. Given the fact that ISPS Code was largely a US initiative, it was not surprising to found that the objectives and contents of the ISPS Code are largely equivalent to the US Maritime Transportation Security Act (MTSA) adopted in 2002.

The ISPS Code consists of two main components. Part A provides the minimum mandatory requirements that ships (and their respective companies) and ports (and the Contracting Government) must follow, while Part B provides more detailed, but not compulsory, guidelines and recommendations in the implementation of security assessments and plans. The section outlines of the two parts are largely equivalent, of which Part A mainly illustrates the principles that maritime stakeholders need to follow, while Part B mainly discusses how such principles should/can be put into practice. Within the ISPS Code, three aspects are directly related to port security, namely: (i) changing security levels; (ii) responsibilities of the contracting governments; (iii) port facility security, including the procedures of undertaking Port Facility Security Assessment (PFSA), preparing Port Facility Security Plans (PRSP) and appointing Port Facility Security Officer (PFSO). While the details of the ISPS Code can be found in IMO's website (IMO, 2007), the port security-related aspects are briefly discussed in the following:

- *Changing security levels* - One of the most significant requirements is the introduction of changing security levels. At all times, a security level system (L1, L2 and L3) must be introduced at all ports within the territory of the contracting government, with higher security levels indicate a greater likelihood of occurrence of a security incident, based on an assessment on the degree of credibility, collaboration, specific and imminent nature of the threat information, as well as the potential consequence of such an incident. Similar security level system also exists in ships.

- *Responsibilities of the contracting governments* - Contracting governments should appoint a designated authority (DA) dedicated for port security affairs, while at the same time establish an administrative structure in supporting the DA in carrying out its duties, including local legal backup. In turn, the DA should set security levels in accordance to Part A of the ISPS Code and provide guidance from security incidents taken place in ports, especially necessary and appropriate instructions to affected ships and port facilities in the case of higher security levels (L2 and L3). They are also responsible to approve PFSA reports and PFSP, as well as testing their effectiveness. Finally, contracting governments should also establish the requirements when a Declaration of Security (DoS) is required when ship and port facilities interact.

- *Port Facility Security* - Under the ISPS Code, ports (and their facilities) are required to act in accordance to security levels set by their respective contracting governments, of which the degree of protective measures should be increased with changing security levels in the following security-related issues: performance of security duties, access and monitoring of port facility and restricted areas, supervision of the handling of cargoes and ship's stores and the availability of security communication.

  Apart from daily routine operation, contracting governments (or its designated authorities) must periodically assess port facilities, namely the Port Facility Security Assessment (PFSA), and report the outcomes (or approve the report if done by a separate designated authority). Through an appropriate risk-based methodology, the assessment must at least address the following issues: (i) identification and evaluation of important assets and infrastructure it is important to protect; (ii) identification of possible threats to the assets and infrastructure and the likelihood of their occurrence; (iii) identification, selection and prioritisation of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and (iv) identification of weaknesses, including human factors in the infrastructure, policies and procedures (IMO, 2002b).

  Finally, based on the assessment outcomes, Port Facility Security Plans (PFSP) should be developed for each port facility, with provisions in addressing the three security levels in the issues including: measures to prevent weapons/dangerous devices from being introduced in the port, authorised access to restricted areas, effective security of cargo and cargo-handling equipment and security of security information; procedures in responding to security threats, new/amended security instructions, evacuation, interfacing with ship security activities, periodic review and updating of PFSP, reporting security incidents, audition of the plan and facilitation of shore leave for ship's personnel or personnel change; as well as identification of port security officer and the duties of security-related personnel. The ISPS Code has noted that one single PFSP in covering more than one port facility is possible, provided that the operator, location, operation, equipment and design of these facilities are highly similar to each other.

To execute the above plans, a Port Facility Security Officer (PFSO) should be appointed for each designated port facility (or one PFSO for multi-facilities if they are largely similar to each other). The PFSO is usually selected by the port facility management, subject to the approval of the contracting government before formally appointed. A PFSO is responsible to ensure that the PRSA exercises and PFSP are well-prepared and being carried out effectively. Apart from routine duties, PFSO also needs to make sure that the facilities concerned are secure through inspection and supervision of facilities, the distribution of responsibilities to his/her subordinates, security-related information gathering, as well as managing the training, drilling and exercises on port facility security. Finally, PFSO also acts as the liaison between the contracting government and the shipping companies, often through the Ship Security Officers (SSO) and Company Security Officers (CSO).

Despite the general consensus that port's security is essential in safeguarding maritime security (Mensah, 2003), the IMO has assumed that the responsibility of port security virtually lied within the hands of the public sector, as reflected in its emphasis on the roles of the contracting governments, where they had the final say in virtually all decisions, e.g., the approval of PFSA and PFSP, the endorsement of PFSO appointment, the right to request DoS, reviewing (parts of) the ship security plan in outstanding circumstances, etc. This implies that non-governmental port stakeholders, including terminal operators, would be largely expected to be followers to international standards and government policies, and would play peripheral roles in the development of port (and its facilities) security issues. In some countries, such shortcomings have been addressed through the formation of committees and working groups in port security. In the US, for example, MTSA required the establishment of Area Maritime Security Committee (AMSC) in throughout all US ports to coordinate the activities of all port stakeholders, including public agencies of different levels, as well as the industry, with specific tasks in collaborating on port security plans, so that resources dedicated for security can be more efficiently utilised. Such emphasis on contracting governments also implies the criticality of training capable manpower in dealing with such new requirements effectively, as pointed out by O'Neil (2003) and Zhu (2006).

3. Research Methodology

Given the study nature, apart from documental review, the author had also conducted various semi-structured, in-depth interviews with key stakeholders who play pivotal roles in carrying out port security measures in the port of Hong Kong, including the Marine Department of the HKSAR Government and port facility operators (hereinafter called 'interviewees'). The objective of such interviews was to identify and obtain information which was otherwise unavailable through published sources. Interviews were mainly conducted at interviewees' respective offices between November 2007 and January 2008.

4. Promulgation and Implementation: Port of Hong Kong

The remainder of this paper will focus on how the ISPS Code has been imposed within the port of Hong Kong. This section is divided into three sub-sections, namely: (i) legal document; (ii) administrative structure; (iii) security levels; (iv) control of ships within/intending to enter the port; and (v) port facility security.

4.1. The Legal Document

In Hong Kong, the main legal document in addressing port security issues is entitled as *An Ordinance to implement the December 2002 amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974 and the International Ship and Port Facility Security (ISPS) Code and related provisions in the Convention to enhance security of ships and port facilities, and to provide for incidental or related matters*, or the *Merchant Shipping (Security of Ships and Port Facilities) Ordinance* for short title (CAP582, Ordinance No.: 13 of 2004, thereafter termed as 'Ordinance'). Section 6 of the Ordinance is complemented by an empowering document, entitled *Merchant Shipping (Security of Ships and Port Facilities) Rules* (CAP582A, thereafter termed as 'Rules'). Both documents were signed by the then Chief Executive, Mr. Tung Chee-hwa, and enacted by the Legislative Council (Hong Kong's de facto Parliament) in June 2004.

To fulfil its objective of implementing maritime security issues in accordance to SOLAS Chapter XI-2 and the ISPS Code, in explaining its rules, the Ordinance and Rules often make reference to these two documents. For example, in port facility security, the Rules clearly state that a designated port facility shall comply with regulation 10.1 of Chapter XI-2 of the Convention (Section 23), while references to Part A of the ISPS Code in issues related to port facility security had been made four times (Sections 24, 25, 28 and 29). The major difference, however, lies in the fact that the Ordinance and Rules provide much more detailed information and guidance on how SOLAS Chapter XI-2 and the ISPS Code should be put into practice in Hong Kong with, for instance, procedures on how an approval of a PFSP amendment can be withdrawn by the Director of HKMD (e.g. CAP582A, Section 27), the power and limitations of inspections by HKMD personnel (CAP582, Sections 11, 12 and 13), the possible fines and/or penalties if the port facility management fails to comply with the set standards (e.g. CAP582, Section 13; CAP582A, Sections 28 and 30), as well as the port facility management's appeal procedures against any decisions made by the Director of HKMD (e.g. CA582A, Section 31)

4.2. Administrative Structure

The security administration structure of the port of Hong Kong can be found in Figure 1.

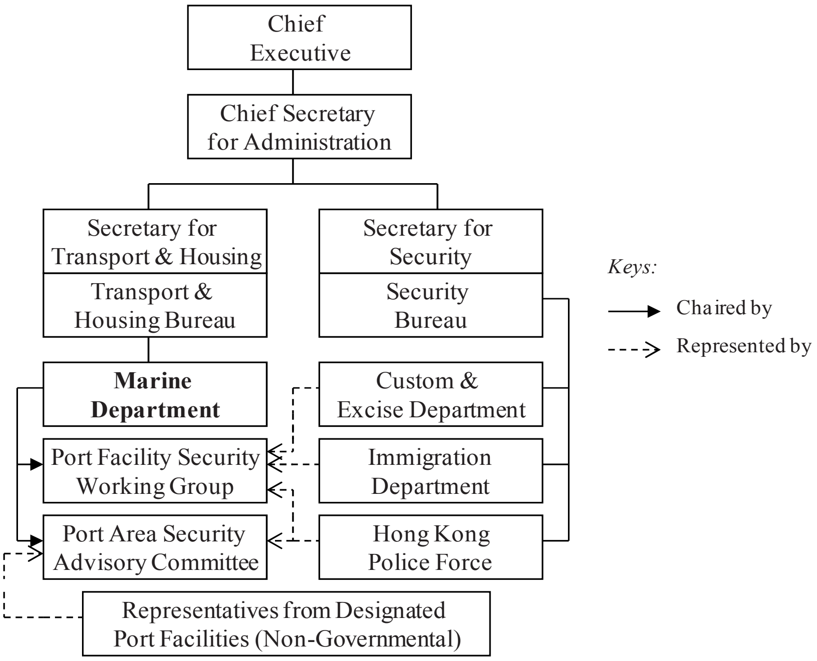

Chief Executive
Chief Secretary for Administration
Secretary for Transport & Housing
Transport & Housing Bureau
Secretary for Security
Security Bureau
Marine Department
Custom & Excise Department
Port Facility Security Working Group
Immigration Department
Port Area Security Advisory Committee
Hong Kong Police Force
Representatives from Designated Port Facilities (Non-Governmental)
Keys:
Chaired by
Represented by

Figure 1: Port security administration structure in Hong Kong in 2008

The Hong Kong Marine Department (HKMD), subordinated to the Transport and Housing Bureau, is the DA for the contracting government, i.e. Government of the Hong Kong Special Administrative Region (HKSAR), in discharging port security duties in accordance to the mandatory requirements of the ISPS Code. According to the Ordinance and Rules, HKMD's Director (hereafter termed as 'Director') may specify the extent of application of SOLAS Chapter XI-2 and the ISPS Code in relation to any designated port facility (Section 5, CAP582), designating security organisations in executing certain port security duties, as long as such organisations possess the appropriate expertise knowledge and not in non-compliance of the Section 4.3, Part A of the ISPS Code, authorisation of officers (Section 9, CAP582) and granting exemptions from the provision of the Ordinance (Section 14, CAP582).

Under HKMD, an advisory, non-statutory committee had been established in June 2003, namely the Port Area Security Advisory Committee (PASAC). The function of PASAC is to advise to the HKSAR government and its designated authority, i.e. HKMD on all matters in connection with the implementation of SOLAS Chapter XI-2 and the ISPS Code in Hong Kong (PASAC, 2003a), as well as to monitor its application in Hong Kong (PASAC, 2004a). In terms of membership, the committee consists of about 20 members chaired by HKMD's Deputy Director, comprised of governmental representatives from HKMD and the Hong Kong Police Force, as well as non-governmental representatives from the designated port facilities Each facility group, e.g. container terminal, bulk terminal, dockyards, etc., will nominate one representative to sit in the committee (PASAC, 2003a). Until November 2007, nine PASAC committee meetings had been conducted. The primary focus of PASAC was on port security (not ship security) while, in some cases, matters related to ship-port interface would also be covered (PASAC, 2003a). The composition of PASAC can be found in Table 1.

Table 1: The composition of PASAC in 2008

Position or Representative	Number
Chairman (Deputy Director of Marine)	1
Secretary (Marine Officer/Port Security Administration)	1
Hong Kong Marine Department (HKMD)	5
Hong Kong Police Force	2
Container Terminal Operators	2
Oil Terminal Operators	2
River Trade Terminal Operators	1
Ship Repairs Industry	2
Cruise Industry	1
Bulk Industry	1
Hong Kong Liner Shipping Association	1
Total	**19**

Source: HKMD website

On July 2003, the Port Facility Security Working Group (PFSWG) was established, chaired by HKMD and represented by the Custom and Excise Department, Immigration Department and the Hong Kong Police Force. PFSWG acts as the executive arm in discharging the obliged duties in sustaining the security of the Port of Hong Kong. The working group is also responsible to evaluate of PFSAs and PFSPs undertaken and prepared by facility operators, before submitting them to HKMD for final approval.

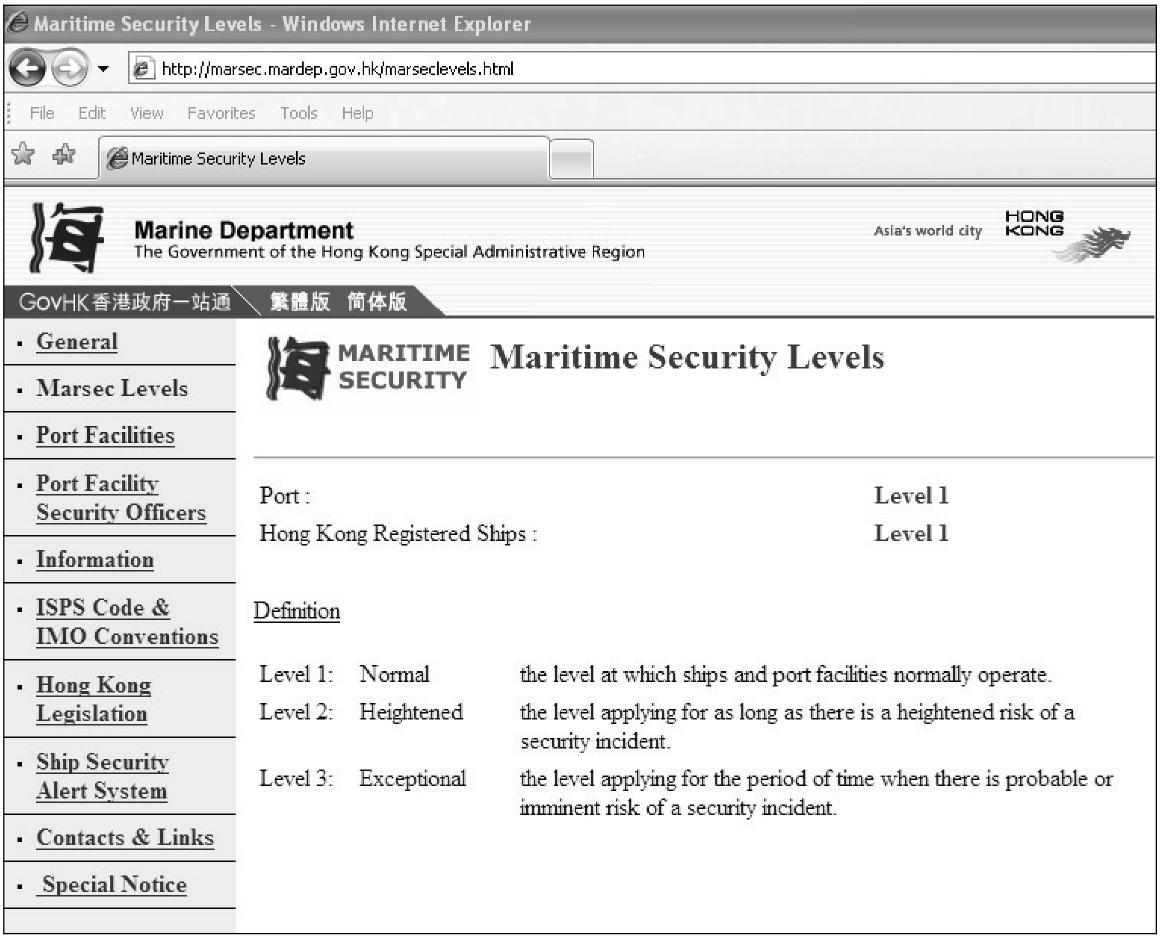
Any port security issues, like new requests from IMO, will be discussed within PFSWG concerning its implications and practicality in Hong Kong and, if found necessary, will be bring up to the agenda of the next PASAC meeting. In most cases, any new amendments, including the Ordinance, the Rules and the details of implementing the articles in IMO's Maritime Safety Committee (MSC) Circulars, will be firstly discussed and compromised within PASAC. According to internal information, although non-statutory in nature, HKMD will always ensure that any new policies would have obtained the endorsement of PASAC before implementation.

In terms of finance, neither the HKMD nor the HKSAR government prepare a budget related to port security, and the income received from the issuance of security certificates and audit exercises are too trivial to cover the administration costs[4]. Also, the companies which own and operate their respective designated port facilities are responsible for all the financial costs in the execution of their respective PFSA, the preparation of PFSP and the actions. During the second PASAC meeting, the chairman had made clear to the facility operators that the government would not subsidise, or provide any loans, to any port security-related projects (PASAC, 2003b).

In general, HKMD is responsible to execute its security obligations in three major categories, namely: (i) setting the security levels; (ii) control of ships within/intending to enter the port; and (iii) port facility security.

4.3. Security Levels

A security level system, L1, L2 and L3, has been introduced, of which the updated status is live on internet, accessible at the HKMD official website 24 hours per day. As illustrated in Figure 2, the definitions of different security levels are equivalent to the guidelines found in Section 1.8, Part B of the ISPS Code.



Maritime Security Levels - Windows Internet Explorer
http://marsec.mardep.gov.hk/marseclevels.html
File Edit View Favorites Tools Help
Maritime Security Levels
Marine Department
The Government of the Hong Kong Special Administrative Region
Asia's world city
HONG KONG
GovHK 香港政府一站通
繁體版 简体版
General
Marsec Levels
Port Facilities
Port Facility Security Officers
Information
ISPS Code & IMO Conventions
Hong Kong Legislation
Ship Security Alert System
Contacts & Links
Special Notice
MARITIME SECURITY

Maritime Security Levels

Port : Level 1

Hong Kong Registered Ships : Level 1

Definition

Level 1:	Normal	the level at which ships and port facilities normally operate.
Level 2:	Heightened	the level applying for as long as there is a heightened risk of a security incident.
Level 3:	Exceptional	the level applying for the period of time when there is probable or imminent risk of a security incident.

Figure 2: An illustration on different security levels in the port of Hong Kong
Source: HKMD website

[4] According to Section 33 of the Rules, HKMD can charge an hourly rate of HKD 1,115-3,270 for services including issuing/endorsing (interim) security certificate, approving PFSP, designated port facility inspections. However, during the fifth PASAC meeting, the chairman had already indicated to committee members that the government had no intention to shift the financial burden of regular security audit exercises to facility operators (PASAC, 2004b).

All information and intelligence related to port security, which can possibly lead to changes in security levels, are provided by the Intelligence Unit of the Hong Kong Police Force. The Police Force will first assess the credibility and potential consequences of the intelligence, before advising HKMD on the necessity to change the security level, of which the website will be updated if a change is confirmed by HKMD[5]. There is a general understanding that the government would instruct a facility operator to close down its facility only when the security level changes to L3, although the ultimate sanction should lie with the DA (PASAC, 2003b).

4.4. Control of Ships within/intending to Enter the Port

The HKSAR government strictly follows the mandatory requirements of international documents in controlling ships within or intending to enter the port of Hong Kong. For example, in the Rules, all the Sections which are related to this issue (Sections 11 and 12, CAP582A) have made full reference to the requirements as indicated in SOLAS Chapter XI-2 (Regulation 9). Any additional regulations on this issue are virtually non-existent. On the other hand, all necessary information and guidelines for ships within/intending to enter the port, including HKMD notices and information notes, pre-arrival security information, DoS and security advice to Hong Kong-registered ships, are easily accessible and downloadable from the internet, through HKMD's website.

4.5. Port Facility Security

Given the traditional port policy of Hong Kong which emphasised on active non-intervention by the public sector (the so-called *laissez-faire* policy), it is not surprising to found that all but three of the designated port facilities are privately owned and operated (the exception being China and Macau Ferry Terminals and Buoys and Anchorage Services, which are operated by HKMD) and the PFSAs and PFSPs are also carried out by these companies (or any recognised security organisation (RSO) chosen by them) themselves, while HKMD takes up the responsibility in undertaking and preparing PFSAs and PFSPs respectively for China and Macau Ferry Terminals as well as Buoys and Anchorage Services. PFSAs and PFSPs will be submitted to PFSWG for evaluation and vetting, before being recommended to HKMD for final approval (Figure 3). Until 2008, HKMD has reviewed and approved 33 PFSPs, consisting of container and ferry terminals, wharfs and dockyards, oil jetty and terminals, power stations, fuel receipt facilities and mooring buoys and anchorages. See Appendix.

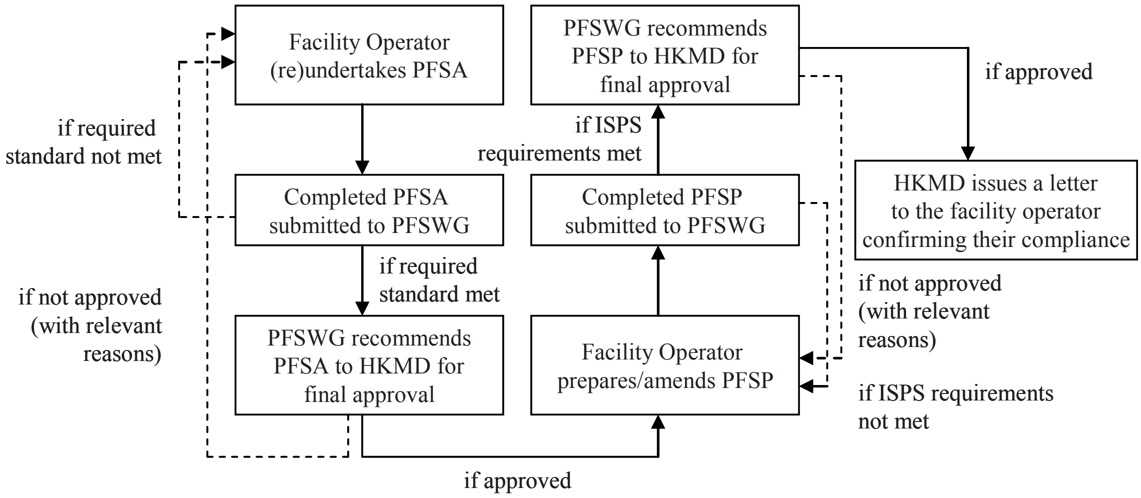

Facility Operator (re)undertakes PFSA
Completed PFSA submitted to PFSWG
PFSWG recommends PFSA to HKMD for final approval
Facility Operator prepares/amends PFSP
Completed PFSP submitted to PFSWG
PFSWG recommends PFSP to HKMD for final approval
HKMD issues a letter to the facility operator confirming their compliance
if required standard not met
if not approved (with relevant reasons)
if required standard met
if approved
if ISPS requirements met
if approved
if not approved (with relevant reasons)
if ISPS requirements not met

Figure 3: Procedures of approving PFSA and PFSP in the port of Hong Kong
Source: Derived from PASAC (2003a)

[5] During the third PASAC meeting, an issue was raised concerning the transmission of threat assessment since the ISPS security levels did not match the conventional security levels used by the Police Force. An *ad hoc* meeting for this issue was conducted at February 2004 between the parties concerned, and had been resolved before the ISPS Code was fully implemented at 1 July 2004.

In compliance to Section 16.8, Part A of the ISPS Code, some companies, notably Hongkong International Terminals (HIT), Modern Terminals Ltd. (MTL) and ExxonMobil (Hong Kong) Ltd., have chosen to prepare a single PFSP for all the terminals that they own and operate[6]. Subsequently, these companies have also chosen to make single PFSO appointment for their respective terminals, as in compliance to Section 17.1, Part A of the ISPS Code. The selection and appointment of PFSOs is decided by the port facility management subject to the formal approval by HKMD. By 2007, 24 PFSOs have been appointed, either as a dedicated position, or undertaken by safety/operation-related managers. HKMD has also ensured that their names and contacts are easily accessible from the internet.

All PFSOs must have received training and certification from a HKMD-accredited local port security programme (or has attended a similar programme overseas, of which verification will be decided on a case-by-case basis) (HKMD, 2007a). In security personnel training and certification, in accordance to Section 4.3, Part A of the ISPS Code, such responsibilities have been fully outsourced to recognised security organisations (RSO), as long as the institution concerned has submitted a proposal to HKMD outlining a programme which fulfils the prerequisites laid down in IMO's Maritime Safety Committee (MSC) Circular No. 1188 (IMO, 2007) and the *Guidelines for Approving PFSO Training Course* (HKMD, 2007b) and a formal accreditation process undertaken by designated HKMD officials[7]. By September 2007, HKMD has approved two maritime institutions in offering security training and certification programmes, while verification of certificates issued by overseas institutions is decided on a case-by-case basis. An example of the contents of a PFSO programme accredited by HKMD can be found in Table 2. The validity of the PFSO qualification is five years, and is renewable subject to the criteria that the personnel concerned had served at least 12 months as (Deputy) PFSO within the validity period (HKMD, 2007a).

Table 2: The modules of a HKMD-accredited PFSO programme in Hong Kong

Module 1	Introduction
Module 2	Maritime Security Policy
Module 3	Security Responsibilities
Module 4	Port Facility Security Assessment
Module 5	Security Equipment
Module 6	Port Facility Security Plan
Module 7	Threat Identification
Module 8	Port Facility Security Actions
Module 9	Emergency Preparedness
Module 10	Security Administration
Module 11	Security Training

Source: Institute of Seatransport (2007)

The major mechanism in auditing the PFSP is through (notified in advance) site visits to the designated port facilities[8], which would tie in with the validity of the Statement of Compliance (SoC) issued (PASAC, 2004b). Auditing is divided into 'full' and 'partial' audits, of which they have to be undertaken at a five- and one-year interval respectively. The auditing schedule and arrangement with the designated security facility management team are arranged by a designated officer from HKMD,

[6] In practice, however, a single security certificate has been issued to each designated facility, so as to ensure that other facilities can still operate normally even when one or more facilities have to close down due to security threats and/or incidents. For example, three security certificates have been issued to MTL's container terminals (DA01, DA02 and DA03, see Appendix), but they are covered and managed by one PFSP and PFSO respectively.

[7] According to the HKMD's *Guidelines for Approving Port Facility Security Officer Training Course*, formal approval to the institution concerned in providing SFSO training and certification would be granted only after the first course of the programme concerned has been monitored and assessed by HKMD officials and the officer(s) concerned, with positive feedbacks.

[8] According to internal information, un-notified inspections cannot be undertaken due to the shortage of financial support from the HKSAR government.

of which the audit team also consists of representatives from the Police Force, Custom and Excise and Immigration Departments[9].

Audit categories are divided into seven areas, namely: (i) documentation; (ii) access control; (iii) handling of cargoes; (iv) port-ship interface; (v) control of restricted area; (vi) awareness; and (vii) security infrastructure. All areas will be examined during a full audit, while four of them will be selected by the audit team leader (usually HKMD's designated marine officer) for each partial audit. According to HKMD, investigating the physical condition of the designated facilities is the most important function during the site visit, of which evaluation results, recommendations and mandatory actions will be laid down in a confidential audit report. In auditing the 'soft' aspects, like personnel arrangement and documentation, the designated facility management needs to fill in a dedicated questionnaire prepared by HKMD.

Minor deficiencies which are unlikely to seriously threaten the designated facilities in complying with SOLAS Chapter XI-2 (like worn-out fencing and non-adequate lighting), Part A of the ISPS Code, the Ordinance and the Rules, will not affect the endorsement of the validity of the security certificate. However, during the site visit, the facility management needs to provide a binding promise to the audit team on when they can rectify the problem(s), and defected facilities will be re-inspected during the next auditing exercise, of which HKMD would void the validity of the facility's security certificate if the non-compliance persists (PASAC, 2004b).

5. Discussions

From the above analysis, it is recognised that several characteristics existed. On a positive note, the port of Hong Kong has mostly, if not fully, fulfilled the mandatory requirements as laid down in SOLAS Chapter XI-2 and Part A of the ISPS Code. Virtually all the core elements of the international mandatory requirements have been addressed, while necessary security information to maritime stakeholders and the public are easily accessible. The HKSAR government is also able to provide a well-supported legal and structural backup in facilitating the implementation of international requirements in Hong Kong and the basic mechanisms in complying with the international requirements are in place. Facility operators are also, in general, quite cooperative with the designated authority in complying with the mandatory requirements from SOLAS Chapter XI-2 and the ISPS Code.

Despite such effectiveness, however, constructive innovation in the implementation of port security issues is rather limited. The local legal documents, i.e. the Ordinance and Rules, had been made as simple as possible, with all the core sections actually confirming that the necessity of implementing the international prerequisites in the port of Hong Kong. Additional security requirements and measures are virtually non-existent, not helped by some local situations which have practically disabled Hong Kong to carry out security-related innovative activities. For example, until now, the port of Hong Kong is still unable to introduce biometric identity system on port workers (which had been carried out in many US and some European ports) because Hong Kong does not have any significant labour unions, while it is not compulsory for workers to join/register for any labour unions. Another example lies in the difference in legal system between Hong Kong and the US. Under Hong Kong's legislation, the designated authority, i.e. HKMD, is not empowered to shut down any port facilities directly, but through providing directions to the non-complying facility to rectify the deficiencies, and even if this is not followed, HKMD could only shut down the facility through withdrawing security certificate and report it to IMO (PASAC, 2006). This implies that the port of Hong Kong is potentially less immediate in reacting to extraordinary, and requiring immediate actions,

[9] According to interviewees, while the Police Force will always send representatives to the audit team, Custom and Excise and Immigration Departments will only send representatives to selected designated facilities of which they are interested. Generally speaking, Custom and Excise Department is only interested in cargo-related facilities, while Immigration Department is only interested in passenger-related facilities.

security incidents like L3, of which in this situation the occurrence of security incident is likely to be imminent.

Furthermore, while fully acknowledging the public nature of port security, at the same time, it is quite clear that the HKSAR government is trying hard to keep port security issues parallel to the city's traditional *laissez-faire* policies in port operation and governance. Apart from the compulsory obligations as laid down in Section 4.3, Part A of the ISPS Code, nearly all the optional responsibilities, including the execution of PFSA (Section 15.2), preparation of PFSP (Section 16.1.1), appointment of PFSO (Section 17.1) and training and certification (Section 18), have been outsourced to RSOs through legislations (like Sections 25 and 26 of CAP582A) and practical means, while the government also resists to recommend any RSOs and thus operators are completely free to choose their own RSOs (PASAC, 2003a). Moreover, as mentioned, the government insists on its non-subsidising policy to any security related projects for any designated facilities (PASAC, 2003b) and does not even allocate any significant financial resources in carrying out port security. Thus, the extent of which port security measures can be implemented in the designated facilities very much depends on the attitude of facility operators.

Given the fact that Hong Kong has yet experienced any changes in its security level from L1 or experiences any significant security incidents (until the end of 2007), Hong Kong is largely considered as a low-risk port with little chance from terrorist attack (PASAC, 2003b). It is therefore not surprising that both the government and designated facility operators are also not very enthusiastic in the idea of investing heavily in security-related projects other than fulfilling the basic mandatory requirements[10]. For example, according to a HKMD's senior marine officer who is actively involved in port security, during the discussion of implementing any new security requirements (either from IMO or the HKSAR government), the core discussion point between PASAC often lies in the financial obligations that facility operators need to devote, where significant gap often exists between public and private expectations. The unwillingness of the government to significantly finance the issue has also further added to the difficulty in becoming an innovator in port security, as exemplified by the fact that HKMD does not even possess the necessary resources in carrying out any additional (un-notified in advance) facility inspections other than routine annual audits, not to mention any potential opportunities for research and development. Indeed, the experience of Hong Kong in complying with security instruments is not completely dissimilar to many other global regions, like Asia and even the European Union, of which stakeholders often feel discontent with the imposition of further rules based on security issues (for instance, see: Ng and Gujar, 2008; Pallis and Vaggelas, 2008).

6. Conclusions

The outbreak of 9/11 terrorist attack has exposed the potential brittleness of the transportation system which can lead to unprecedented disruption of the global trade system. In responding to such challenge, various security enhancement instruments have been introduced by the international community, notably the ISPS Code. Although a number of works on maritime security had been carried out, works dedicated to port security, including globally important economic regions in Asia, remained scarce, where comprehensive review on how such international guidelines can be applied in a local perspective is clearly lacking. Understanding this, through studying the port of Hong Kong, this paper critically reviews on how the international requirements, i.e., the ISPS Code, have been implemented on a local region.

Based on this paper's analysis, it is found that Hong Kong is largely a 'follower', rather than an 'innovator', in dealing with port security issues. The port security administrative structure is

[10] According to anecdotal information from interviewees, the fact that Hong Kong is part of China, of which China, in general, maintains rather friendly relationship with most Middle Eastern countries/regions, has also strengthened the 'safe image' of the port of Hong Kong, which has further discouraged any additional financial incentives to enhance security in designated port facilities.

fundamentally a designated authority purely for the implementation of SOLAS Chapter XI-2 and the ISPS Code with virtually no innovation at all. Also, from the above analysis, it seems that security issue is not widely regarded as an important issue in port operation in Hong Kong. Indeed, such perception is reflected by the fact that, as confirmed by various interviewees, in many port facility operating companies, the PFSO (or security manager) is often a rather junior position within the company, while the government, as mentioned, is quite reluctant to input resources of any significance into addressing the issue. Contrary to the major American and some Western European ports (notably Rotterdam), a 'security culture' has yet to establish in the port of Hong Kong. Indeed, from author's self-observation, the core rationale of compliance by Hong Kong maritime stakeholders seems to be avoiding potential economic loss due to non-compliance (like losing the American market), rather than appreciating the concept of 'more secured port'. In other words, port security is more a problem to solve rather than an opportunity to innovate. Indeed, the port of Hong Kong can partly reflect the situation of Asian ports, where the approach of carrying out port security measures is rather half-hearted, pro-trade and economically driven (Ng and Gujar, 2008).

Conclusively speaking, the case studied in this paper illustrates that rules and standards may not be completely effective, where local circumstances and other software aspects (like attitudes and governance system) should not be overlooked if port (and indeed maritime and supply chain) security can be carried out effectively. Further research is required to investigate how such obstacles can be effectively overcome. Last but not least, by undertaking a detailed investigation on the imposition of port security measures in a local perspective, this paper has provided valuable insight on the problems, obstacles and solutions in applying maritime security measures to different global regions, as well as a decent platform for further research on this increasingly important, but understudied, topic.

7. Acknowledgements

The author would like to thank all the interviewees and anonymous reviewers who have provided useful information and comments to this paper. All errors and omissions remain the sole responsibility of the author.

References

APEC (2002), APEC 2002 Leader's Declaration, The Tenth APEC Economic Leaders' Meeting, Los Cabos, Mexico, 27 October, accessible at: http://www.apec.org/apec/leaders__declarations/2002.html.

APEC's official website: http://www.apec.org, last accessed on February 2008.

Asia Pacific Foundation of Canada (2004), New security measures challenge competitiveness of Asian ports, Asia Pacific Bulletin, 30 April, accessible at: http://www.asiapacificbusiness.ca.

Bichou, K. (2004), The ISPS Code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management, Maritime Economics and Logistics 6: 322 – 348.

Bichou, K., Bell, M.G.H., and Evans, A. (eds.) (2007), Risk Management in Port Operations, Logistics and Supply Chain Security, London: Informa LLP.

Flynn, S.E. (2006), Port security is still a house of cards. Far East Economic Review, Jan/Feb 2006, accessible at: http://www.feer.com/articles1/2006/0601/free/p005.html.

Greenberg, M.D., Chalk, P., Willis, H.H., Khiko, I. and Ortiz, D.S. (2006), Maritime Terrorism: Risk and Liability. Santa Monica: RAND Corporation.

HKMD website: http://www.mardep.gov.hk, last accessed on March 2009.

HKMD (2007a): Guidelines for Application of Qualification Recognition as Port Facility Security Officer. Accessible at: http://marsec.mardep.gov.hk/pfso_training.html.

HKMD (2007b): Guidelines for Approving Port Facility Security Officer Training Course. Accessible at: http://marsec.mardep.gov.hk/pfso_training.html.

Hong Kong Institute of Seatransport (2007): Port Facility Security Officer Course. Hong Kong: Institute of Seatransport.

Huxley, T. (2005), Southeast Asia 2004 stable, but facing major security challenges, In: K.W. Chin and D. Singh (eds.): Southeast Asian Affairs 2005, Singapore: Institute of Southeast Asian Studies, pp. 3-23.

IDSS (2004), Maritime Security in the Asia-Pacific: Report of a Conference Organized by the Institute of Defence and Strategic Studies (IDSS), held in Singapore, 20-21 May.

IMO (2002a), Amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974 as Amended. London: International Maritime Organisation, SOLAS/CONF.5/32, December 2002.

IMO (2002b), International Code for the Security of Ships and Port Facilities (ISPS Code). London: International Maritime Organisation, SOLAS/CONF.5/34, December.

King, J. (2005), The security of merchant shipping, Marine Policy 29: 235-245.

Kumar, S.H. and Vellenga, D. (2004), Port security costs in the US: a public policy dilemma, Proceedings of the Annual Conference of the International Association of Maritime Economists, Izmir, Turkey, July.

Mensah, T.A. (2003), The place of the ISPS Code in the legal international regime for the security of international shipping, WMU Journal of Maritime Affairs, 3(1): 17-30.

Ng, K.Y.A. (2007), Port security and the competitiveness of short sea shipping in Europe: implications and challenges. In: Bichou, K., Bell, M. and Evans, A. (eds.): Risk Management in Port Operations, Logistics and Supply Chain Security. London: Lloyd’s of London Press and Informa, pp. 347-366.

Ng, K.Y.A. and Gujar, G. (2008), Port security in Asia, In: W.K. Talley (ed.): Maritime Safety, Security and Piracy. Informa LLP, London, pp. 257-278.

O’Neil, W.A. (2003), The human element in shipping, WMU Journal of Maritime Affairs, 2(2): 95-97.

OECD (2003), Security in Maritime Transport: Risk Factors and Economic Impact, Paris: OECD Maritime Transport Committee.

Pallis, A.A. and Vaggelas, G.K. (2007), Enhancing port security via the enactment of EU policies, In: Bichou, K., Bell, M. and Evans, A. (eds.): Risk Management in Port Operations, Logistics and Supply Chain Security. London: Lloyd’s of London Press and Informa, pp. 303-334.

Pallis, A.A. and Vaggelas, G.K. (2008), EU port and shipping security, In: Talley, W.K. (ed.): Maritime Safety, Security and Piracy. Informa LLP, London, pp. 235-255.

PASAC (2003a), Minutes of the First Meeting of the Port Area Security Advisory Committee. Hong Kong: Hong Kong Marine Department (July 2003).

PASAC (2003b), Minutes of the Second Meeting of the Port Area Security Advisory Committee. Hong Kong: Hong Kong Marine Department (September 2003).

PASAC (2004a), Minutes of the Fourth Meeting of the Port Area Security Advisory Committee. Hong Kong: Hong Kong Marine Department (May 2004).

PASAC (2004b), Minutes of the Fifth Meeting of the Port Area Security Advisory Committee. Hong Kong: Hong Kong Marine Department (September 2004).

PASAC (2006), Minutes of the Eighth Meeting of the Port Area Security Advisory Committee. Hong Kong: Hong Kong Marine Department (October 2006).

Pilling, D. and Mitchell, T. (2006), US official urges Asia to improve port security, Financial Times, 28 March.

Pinto, C.A., Rabadi, G. and Talley, W.K. (2008), US port security, In: Talley, W.K. (ed.): Maritime Safety, Security and Piracy. Informa LLP, London, pp. 217-233.

Robinson, R. (2002), Ports as elements in value-driven chain systems: the new paradigm, Maritime Policy and Management, 29(3): 241-255.

Tan, A.T.H. (2005), Singapore's approach to homeland security, In: K.W. Chin and D. Singh (eds.): Southeast Asian Affairs 2005. Singapore: ISAS, pp. 329-362.

W.K. Talley (ed.) (2008), Maritime Safety, Security and Piracy, London: Informa LLP.

Zhu, J. (2006), Asia and IMO technical cooperation. Ocean and Coastal Management 49: 627-636.

Appendix: Designated port facilities of which PFSPs have been reviewed and approved by Marine Department, HKSAR Government

PFSP Approved:*

DA01	Container Terminal 1, Modern Terminals Ltd.
DA02	Container Terminal 2, Modern Terminals Ltd.
DA03	Container Terminal 5, Modern Terminals Ltd.
DA05	Container Terminal 4, Hongkong International Terminals
DA06	Container Terminal 6, Hongkong International Terminals
DA07	Container Terminal 7, Hongkong International Terminals
DA08	Container Terminal 9 (North), Hongkong International Terminals
DA09	Container Terminal 8 (East), COSCO-HIT Terminals (Hong Kong) Ltd.
DA10	Container Terminal 3, CSX World Terminals Hong Kong Ltd.
DA11	Container Terminal 8 (West), Asia Container Terminals Ltd.
DA12	Ocean Terminal, Harbour City Estates Ltd.
DA13	Hongkong United Dockyards, Hongkong United Dockyards Ltd.
DA14	Lok On Pai Oil Jetty, Hong Kong Petrochemical Company Ltd.
DA15	Shiu Wing Steel Wharf, Shiu Wing Steel Ltd.
DA16	Castle Peak Power Station Coal Unloading Jetty, Castle Peak Power Co. Ltd.
DA17	Green Island Cement Wharf, Green Island Cement Company Ltd.
DA18	ExxonMobil Oil Terminal East, ExxonMobil Hong Kong Ltd.
DA19	ExxonMobil Oil Terminal West, ExxonMobil Hong Kong Ltd.
DA20	Aviation Fuel Receipt Facility, AFSC Operations Ltd.
DA21	Lamma Power Station Coal Unloading Jetty, Hongkong Electric Co. Ltd.
DA22	China Ferry Terminal, Marine Department, HKSAR Government
DA23	Macau Ferry Terminal, Marine Department, HKSAR Government
DA24	Container Terminal 9 (South), Modern Terminals Ltd.
DA25	Government Mooring Buoys & Anchorages, Marine Department, HKSAR Government
DA26	River Trade Terminal, River Trade Terminal Company Ltd.
DA27	Towngas Wharf - Tolo Harbour, The Hong Kong and China Gas Co. Ltd.
DA28	Chevron Oil Terminal, Chevron Companies (Greater China) Ltd.
DA29	Shell Oil Terminal, Shell Hong Kong Ltd.
DA30	CRC Oil Terminal, China Resources Petrochems (Group) Co. Ltd.
DA31	Euroasia Dockyard, China Merchants Container Services Ltd.
DA32	Yiu Lian Dockyards, Yiu Lian Dockyards Ltd.
DA33	China Merchant-Wharf, China Merchant Godown, Wharf & Transportation Co. Ltd

* DA04 (MTL Terminal 8 (West)) was cancelled because MTL had transferred the terminal's ownership to ACT and thus had been inscribed into ACT Terminal 8 (West), i.e., DA11

Source: HKMD website