

**OPENING ADDRESS BY RADM LUI TUCK YEW  
CHIEF EXECUTIVE  
MARITIME AND PORT AUTHORITY OF SINGAPORE  
AT THE OPENING OF THE  
INTERNATIONAL MARITIME & PORT SECURITY  
CONFERENCE (IMPSC) 2004  
GRAND COPTHORNE WATERFRONT HOTEL  
WEDNESDAY, 4 AUGUST 2004**

Good morning, Mr. Yeo Cheow Tong, Minister for Transport,  
Distinguished Guests, Ladies and Gentlemen,

1 Thank you Minister for your thoughtful and thought-provoking remarks. Please allow me to add my welcome to that given earlier by the Minister for Transport. It is my great pleasure to join you this morning at the second International Maritime and Port Security Conference organised by the Maritime and Port Authority of Singapore and IBC. I am encouraged by the response from a broad cross section of the international maritime and security communities. I am confident that we will have a professionally enriching time together over the course of the next 2 days.

ISPS Implementation

2 The first IMPSC was held in January 03, barely a month after the IMO adopted the International Ships and Port Facilities Security Code or the ISPS Code for short. We recognised then the importance and global implications of the code across the entire

spectrum of maritime commerce and the need to take early and decisive steps given the tight implementation timeline

3 Today, some 18 months later, we gather to take stock of the implementation of the ISPS code a month after its entry into force on 1 July 2004 and to look ahead as we consider the additional steps the global maritime community can take to enhance security while continuing to facilitate global trade and commerce.

4 Before we do so, I would like to take a few moments to summarise the implementation of the ISPS code in Singapore, as a global hub port and major flag state. We knew that among the critical first steps were to mobilise the entire maritime and security community in Singapore into action, communicate the requirements of the ISPS code and identify and certify the training providers and the Recognised Security Organisations. Following the 1<sup>st</sup> IMPSC, MPA continued to organise a series of seminars to educate and inform the local maritime community. We worked closely with the port facility operators, ship owners and their representatives for early submission and simultaneous implementation of security plans. We monitored very closely the progress of implementation, checking on a weekly and sometimes daily basis with the RSOs, facility operators and ship owners while identifying and resolving critical bottlenecks. The wholehearted support and participation of various agencies from the Home Team and the Republic of Singapore Navy were instrumental in the thorough assessment and audit of the various plans. Our ports and Singapore flagged ships complied early and successfully with the ISPS code. A few ships which had been undergoing extended

repairs in shipyards or were at sea prior to 1 July 2004 were certified shortly thereafter.

5 We were also concerned with the potential disruption to port and shipping operations. The early signs were not promising. Checks with IMO showed that the pace of progress was slow. We decided that as a global hub port, we should do our part to incentivise early compliance by ship owners and operators. Our contribution to this endeavour was to grant an additional 5% discount on port dues for all ships calling at the port of Singapore in the months of May and June with valid International Ship Security Certificates onboard. It would be a small yet symbolic gesture to recognise those who had made the effort to fulfil their obligations ahead of time. In doing so, we would also benefit by building up a database on the ships which had complied early, thereby easing the load on our inspectors post 1 July. I am pleased to report that the implementation of the ISPS code did not disrupt trade and commerce in Singapore and I understand that worldwide, there had only been minimal disruptions.

#### ISPS Maintenance and Improvement

6 Moving ahead, we need to ensure that we continue to maintain and improve on these efforts to conform to the security requirements of the ISPS code. Onboard ships and in facilities ashore, crews change, vigilance is dulled over time, readiness levels plateau and may even start to decline as attention and emphasis are shifted to other areas. We cannot permit our hard-earned gains in security readiness to be eroded with the passing of time.

7 Maritime security training and audits in the form of realistic exercises and drills is key to ensuring the continuous and effective implementation of the ISPS Code in the world's merchant fleet and port facilities. Readiness needs to be tested, loopholes need to be identified and closed, best practices need to be shared and disseminated. Plans atrophy if they remain on paper, untested and unchecked. Planners need to be nimble and refine their security plans from time to time – we cannot afford to be unchanging and unmoving. Testers and auditors need to be rigorous, creative yet flexible in approach – we cannot afford to be unquestioning and unyielding. Otherwise, the investments in maritime security we have made so far will come to naught and we run the risk that all will come undone.

8 In our business, there is no room for complacency. Out at sea, a bad day on the wrong day can be our last day. It is a common saying that failure can be the first step toward success. I believe that equally so, success can be the first step toward failure, if we allow complacency to set in. In implementing ISPS as successfully as the global maritime community has done in the short span of 18 months, we can all take a moment to savour the sweet scent of success. But let it be only a short moment less it intoxicates us.

### Beyond ISPS

9 As pointed out by Minister Yeo earlier, we need to take cognisance that there are other important facets of maritime security which were not addressed in the implementation of the

ISPS Code. I will summarise it as the need to go smaller, the need to go deeper and the need to look closer at people.

### The Need to go Smaller

10 The requirements of the ISPS Code only applies to ships which trade internationally and are above 500GT. Yet, we have seen that the attacks on *USS Cole* in October 2000 in Aden and the French tanker *Limburg* off the Yemeni coast in October 2002 were carried out by small vessels, plying close to the coastal areas. The lesson is obvious - small boats can equally pose a security threat, particularly in a target-rich environment within or close to the congested confines of port waters or restricted waterways.

11 There are about 3,000 small vessels operating in the port of Singapore. These vessels include the port limit tankers, passenger launches, tug boats and barges that serve the bigger cargo and passenger ships as well as pleasure craft. As a start, we have developed a set of security guidelines that we expect these smaller vessels to abide by. Over time, we hope to make greater use of available technology to give us a better situation picture of vessels, both large and small, in and around our waters. In support of the security agencies, the MPA is testing a low-cost transponder system, which we called HARTS or Harbour Craft Transponder System, for eventual installation on those ships that are excluded from the SOLAS regime. The HARTS is the low-cost cousin of the AIS transponders that ships of 300 GT and above need to install under IMO regulations. Together with the AIS, the HARTS program, if successful, will enable us to monitor, identify and track

almost all craft and vessels that ply in our port and allow the security agencies to focus their inspections and attention on those that do not carry an electronic identification code.

### The Need to go Deeper

12 Thus far, we have focussed on taking steps to secure ships and port facilities. However, we also need to consider the cargo which they carry and the process through which the cargo is assembled and containerised. Let me share some thoughts on this.

13 The Container Security Initiative of the United States is a useful start. The next step is to delve deeper and focus on content security, on what is inside rather than on the box itself. To address this, there are two key elements to consider in strengthening the security of the cargo supply chain.

14 The first is information sharing. Information about the nature, origin, transport and destination of cargo is important for risk-profiling of suspicious cargoes in the supply chain. Risk-profiling is the core element of a focussed approach to identify high-risk cargo and targeted action without undue disruption to trade flows. The greater the awareness we have of cargo and its movement in the supply chain, the better our chances to identify patterns, anomalies and deviations from the norm. Likewise, the need to identify anomalies and deviations apply equally to ships. If we are able to spot aberrations in trading patterns or identify journeys where we are unable to account for a significant portion of a ship's time at sea, these could be factored into the targeting matrix for port state

control inspections. To return to the topic of cargo or content security, the World Customs Organisation (WCO) has embarked on developing standards on supply chain security, and information sharing should be a critical component of the standards being developed.

15 The second element to supply chain security is that a holistic approach is needed to take into account key processes as well as players in the chain. In terms of processes, supply chain security entails devising security measures that could cover activities carried out at the point of origin, and this includes, assembling, packaging and stuffing to the final discharge of the goods. Tracking of containerized cargo onboard ships and in transshipment ports is not a panacea if the start point of stuffing containers is unsecured in the first place.

16 Supply chain security also requires every player related to the delivery of the cargo – manufacturers, forwarders, shippers, port authorities - to play their part in ensuring the security of the cargo. We need to do more to engage the manufacturers, forwarders and shippers so they can play their rightful roles to safeguard against the threats to transport security.

#### The Need to Look Closer at People

17 Seafarers are allies in the fight against terrorism. In fact, they are part of the group of frontline warriors whose vigilance onboard a vessel, whether at sea or alongside, is crucial. Unfortunately, they are viewed in some quarters as potentially the cause rather than a cure of security related problems. We cannot alienate an

important ally by treating all visiting seafarers as potential terrorists. To do so risks generating widespread ill-feeling among the very constituents who play such an important security role and would be counterproductive to our security goals.

18 Yet, we need to be mindful of the legitimate security concerns of countries which may hold this view.

19 I believe there are lessons we can learn here from the aviation industry. The treatment for aircrew is quite different from that for seafarers. There are a variety of reasons but In part, I attribute it to confidence generated by the hiring process. The aviation industry exercises greater scrutiny over who it hires. This extends from the pilots and stewardesses to the technicians on the ground responsible for turning around and maintaining an airplane. Recently, even baggage handlers, screeners and other ground staff are subjected to more detailed background checks.

20 For seafarers, the Seafarer Identification Document (SID) is a step in the right direction. It puts a face and a name to an individual. Yet, it doesn't quite solve a fundamental concern; it doesn't tell you enough about the background of an individual. This requires a different process altogether. I have been thinking, and I add the caveat that these are personal thoughts, about the roles of crewing agencies and the part they play in the recruitment and selection of seafarers and the complementary role of shipmanagement companies in this procedure. We need to engage these parties and if necessary, to even consider an accreditation process for crewing agencies so we can have greater



confidence that the right people are entering our industry. We pay much attention to the training of seafarers and rightly so, given the responsibilities that we entrust them with. It may be that we need to pay as much attention to who we hire as we do to training them.

#### Concluding Comments on IMPSC

21 The maritime industry has risen to the challenge of complying with the ISPS Code adopted 18 months ago. The first IMPSC held last year brought together the experts from the different countries to prepare the international maritime community to implement the ISPS Code. I believe that the conference had helped in some ways to facilitate the smooth implementation of the ISPS Code.

22 There will be other challenges ahead, post-ISPS and beyond ISPS. My hope is that this 2nd IMPSC will see us benefiting once again from the various speakers and experts, offering a diversity of views and thoughts so that we can begin to think deeply about the possible maritime security challenges that will confront us in the years to come. On this note, I wish all of you a very fruitful conference.