Port Marine Security and Counter Terrorism 2006 Conference

Maritime Security: A Shipping Industry Perspective

18 May 2006, Sydney

Address by Mr Michael Phillips, Chairman of Shipping Australia Limited

Introduction

It is intriguing to the casual observer to note that as we get further and further away from 9/11, the Bali, Madrid and London bombings, the introduction of terrorist measures continues, building layer upon layer of regulation. Being cost recovered from industry, one of the normal checks on increased Government regulation ie. where the Government pays, has been removed.

There is a regrettable tendency for the regulators to continually to want to introduce new measures and tighten existing ones in order to be seen to be fulfilling their role and functions.

Whilst this is generally overt there is also a covert aspect with existing border agencies such as Customs, more strictly interpreting the rules and regulations in the name of security when there has been no identified increase in the risk, thereby adding costs and inefficiencies to our collective trade facilitative efforts.

Whilst the expressed objective is to introduce measures commensurate with the identified risk which emerges from threat identification and to ensure minimum disruption to trade, we must all be on our guard to ensure that the continuing anti-terrorism measures meet that criteria.

First up, I wish to set the scene and then I am going to make a number of comments from a shipping industry perspective on:

a. future container supply chain security
b. recent security initiatives that involve advanced technology
c. the Maritime Security Identification Card and seafarer identification.
d. Who pays?

The Maritime Transport Security Act (MTSA) came into force on 1 July, 2004. But the world of security regulation doesn't stand still for very long. Since July 2004 there have been a number of reviews and other drivers for change to the maritime security regime – including the Secretaries Committee on National Security review of maritime security, the Taskforce on Off-shore Maritime Security, ongoing minor reforms in terms of the international regime set out in the IMO SOLAS Convention, and also some fine tuning following experience with implementation of the regulations.

Such is the pace of change that the MTSA didn't last a year before it was changed to the Maritime Transport Off-shore Facilities Security Act – to reflect the extension of

the maritime security regime to Australia's offshore oil and gas facilities. These facilities have submitted plans setting out the preventative security arrangements similar to the International Ship and Port Security (ISPS) Code and these new arrangements were implemented from 30 September last year.

A key component of the regime has been the establishment of maritime security zones. These zones have been established in Australian ports, and on Australian regulated ships, in accordance with maritime and ship security plans. Maritime security zones are areas of special security significance which warrant special protection – unauthorised access to a maritime security is an offence carrying 50 penalty points which at the moment amounts to $5500 for a natural person.

The maritime security regime is also being reformed outside the port environment. The IMO is currently considering amendments to the SUA Convention and its Protocol relating to fixed platforms. The full title for the SUA Convention is the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988. The original SUA Convention provided a mechanism for dealing with crimes at sea – but it didn't deal with terrorism at sea, and it was recognised after September 11 that this needed to be addressed. SUA is being revised to include new offences for terrorist acts including:

- unlawfully, intentionally and for terrorist purposes using against or on a ship or discharge from a ship any explosive, radiological material or prohibited weapon in a manner that causes or is likely to cause on or off the ship, serious injury or damage

- discharging from a ship oil, liquefied natural gas or other like substances in such quantity or concentration that causes or is likely to cause serious injury or damage

- using a ship in a manner that causes or is likely to cause serious injury or damage.

The SUA is also being revised to include offences for unlawfully and intentionally transporting weapons of mass destruction including nuclear, biological, or chemical weapons.

Importantly the SUA amendments will permit the boarding and search of vessels beyond the limits of the territorial seas (on high seas or in the EEZ) if such vessels are reasonably suspected to be involved in offences under the Convention – but such boarding and search provisions are premised on flag state consent and consistency with the UN Convention on the Law of Sea (UNCLOS).

The MUA has been concerned with the shipping of High Consequence Dangerous Goods under Coastal Voyage Permits ie. by non-Australian licensed vessels but the developments with the SUA Convention should give them some comfort. Furthermore, the risk of, for example, carrying ammonium nitrate is not onboard the vessel but rather when it is transported on land. Again assessment of the actual risks involved must be carefully assessed.

Another issue for ships on the high seas is long range identification and tracking. A proposal for a mandatory international system of tracking SOLAS ships has been an issue debated at the IMO, and further work is scheduled which could see a new SOLAS regulation to be implemented late in 2006. There are still a large number of issues to be resolved in terms of coming to international agreement on how such a worldwide scheme could be implemented.

Another significant change to the security environment for ships at sea in Australia's region is that the ADF has been formally charged with responsibility for off-shore counter-terrorism prevention, interdiction and response. The Joint Off-Shore Protection Command (JOPC) has been created (ADF and Customs) and the Australian Maritime Identification System (AMIS) of ship reporting has been implemented.

The Future of Supply Chain Security

It is noted that so far, increased security in the maritime industry in Australia has concentrated on security regulated ports and ships rather than tackling what is a very difficult issue and that is supply chain security.

I believe that technology will play an increasingly important role in enhancing container supply chain security, in particular and the earliest possible advice of the contents of containers being imported into Australia will also assist in the risk assessment process. As a result of the Secretaries Committee on National Security's deliberations, the Government provided funds to increase the level of Customs x-raying of containers from 5% of inward containers to 7% in the main capital city ports and this has been implemented. Such containers are selected based on predetermined criteria in other words it is not a random selection although some export containers and some empty containers may be x-rayed from time to time. A concern of the importer industry has been the imposition of storage charges by container terminals when import containers have been late due to x-raying.

Many trucks are now tracked by GPS receivers using Intelligent Transport Systems and the question has been raised whether containers could be similarly tracked or whether we should advocate the increasing use of smart containers which could be tracked and any evidence of tampering could potentially be shown on a computer screen. What we are really interested in tracking is consignments rather than the package which is the container. We need to be sure that what is being imported into Australia is what is stated on the manifest and that we are aware of its origin even though it may be a transhipped container and the origin may not be readily apparent. The debate within the World Customs Organisation on the 35 digit Unique Consignment Reference number (UCR) offer a way forward in terms of tracking consignments and it should be supported by the Australian Government.

In addition the WCO policy making body, the Council, at its meeting in June last year agreed on a framework of standards to secure and facilitate global trade. The framework aims to:

- establish standards that provides supply chain security and facilitation at a global level to promote certainty and predictability

- enable integrated supply chain management for all modes of transport
- enhance the role, functions and capabilities of Customs to meet the challenges and opportunities for this century
- strengthen cooperation between customs administrations to improve their capability to detect high risk consignments, strengthen Customs/business cooperation and promote the seamless movement of goods through secure international trade supply chains.

Included in the requirements is a proposal that containers be screened as early as possible in the supply chain at or before the port of departure. This raises the question of whether the requirements by the US and Canada to have reported certain information fields on containers 24 hours prior to loading in the exporting countries for containers to or transiting North America should not be applied more broadly.

We would urge the Australian Government to discuss with our major trading partners (outside North America) the possibility of such advanced reporting being introduced in those countries.

Shipping Australia remains concerned regarding the treatment of High Consequence Dangerous Goods, particularly those being imported into Australia that could be used in a potential terrorist attack. In other words broadening our approach over and above that which has been applied to ammonium nitrate. There is a need for a clear delineation between the responsibilities for border protection of the Commonwealth Government and the regulation by States of the movement of such material within their borders.

Recent Security Initiatives that Involve Advanced Technology

Increasingly, technology will play an important role in assisting with container and seal integrity as it passes through the chain and, as mentioned previously, with the tracking of actual consignments rather than the containers themselves. The use of Radio Frequency Identification Tagging (RFIT) being applied to cargo could assist in this endeavour but there have been serious risks identified with this technology, especially hacking into the system.

Embedded RFID devices not deactivated after sale can allow items to be identified at a later time and, there are major privacy issues in the US with the use of such technology. It is interesting that California earlier this year, banned RFID applications in all State documents.

As technologies develop, however, it can be expected RFID will play a greater role and there are passive RFID seals which are relativity cheap and which can allow remote readers to indicate if the container has been tampered with.

The so-called SMART container will emerge but we must ensure that the technology employed is flexible enough to be relatively easily upgraded because any new technology can quickly become redundant.

There may also be the opportunity for greater technology to be used within secure container terminals in the future, for example with instruments being installed on portainer cranes that could quickly detect any radioactivity, explosive gas or heat emanating from a container. These issues will remain under active consideration as we seek to enhance our security measures within a framework of both cost effectiveness and trade supply chain facilitation.

The Maritime Security Identification Card and Seafarer Identification

The Maritime Security Identification Card again arose from the maritime security review by the Secretaries Committee on National Security and the objective is to ensure that all persons requiring unescorted access or not being continuously monitored while in security regulated areas in ports or within off-shore security zones should be subject to appropriate background checking. This will be achieved via a criminal history check (at least those activities which could have implications in terms of terrorist activities) a security background check by ASIO and at the initial stages of application there is an immigration check.

The relevant regulations came into effect on 1 September, 2005. The rollout commenced later than planned and there are about 90,000 to 130,000 MSICs to be issued by 1 January 2007.

Issuing bodies for MSICs are required to have a security plan which covers all aspects of the operation. Shipping Australia supports this initiative but again it is important that it be implemented in a practical and on a risk assessed basis. Following industry and union representations, the Government decided to remain the vetting agent for determining whether an employee is able to be issued with a card or not. This is important to retain the absolute integrity of the system.

Australian seafarers will require MSICs but not foreign seafarers. The USA has required seafarers visiting the United States to have a valid visa for doing so, having been interviewed at a US consulate office and going through the normal visa process. If that seafarer does not hold such a visa then they are restricted onboard while in port in the US. Similarly, although using an electronic process, the Australian Government announced last December that from 1 July, 2007 Australia would require all foreign seafarers visiting Australia to have a visa for Australia. This is in addition to the existing arrangements whereby there is a requirement for all foreign seafarers to have passports and one other document of identification and face to passport checks are conducted by Customs at the first port of call in at least 80% of cases which would essentially be 100% in all the major ports.

The Government has undertaken to consult Shipping Australia on the details of the new visa scheme but we remain concerned that no other countries besides Australia and the US have this requirement. The danger is every country will have a different process and procedures.

If the ILO Convention 185 on a new seafarer identity document is not adopted internationally and the Australian Government has indicated that it is not inclined to do so for the time being, then our chances of achieving an international standard are slim indeed.

This also raises the prospect of at least some foreign seafarers being denied shore-leave while in Australia which, in turn, could affect the future safe operations of the vessel. Whilst we are assured nationalities of particular interest are not numerous; this could change fairly quickly.

There are a lot of details to be discussed with DIMA eg. the proposed two year validity period for the visa is very short (or sooner if the passport expires). What procedures will apply to seafarers requiring medical attention but they do not have a valid visa? Overall, it is considered that frequent callers will be able to cope but the real problems are going to be experienced in the bulk and tramp trades.

It is also worth noting that the International Chamber of Shipping has been receiving a steady stream of reports from shipping companies on ISPS compliance and has conducted a survey between October 2005 and March 2006 which highlighted areas of concern which, in summary, involved:

- 14 reported instances where port facilities failed in their implementation of the ISPS Code representing over a third of reported deficiencies such as lacking in fundamental security measures (lighting/access controls etc) or the absence of a Port Facility Security Officer (PFSO) and no means of contacting him. In addition, it was found that in some ports the security officer rarely visited ships calling at their facilities. (Of interest, there were two reports where port facilities remained unresponsive to calls for assistance from ships under attack from pirates!)

- Behaviour of shore side facilities was inappropriate in almost 20% of reported deficiencies eg. officials continuing to arrive without notification, refusing to wear visitor identification or sign their names in the visitors book where required by the ship's security plan. There have been instances in the past of this occurring in Australia but not recently.

  These deficiencies reinforce the need to constantly upgrade the global approach to counter-terrorism measures.

Who Pays?

There has been a lot of debate recently regarding the costs of security and is it really what the Government claims the “cost of doing business”? The Australian Government has already allocated over $3 billion for domestic security for 2001 to 2008. This involved strengthening Australia’s intelligence capability, providing additional protective border security and building up our response capability as well enhancing the security capacity in our region. However, many of the maritime security issues are built on a user pays system and there is the real danger of regulatory creep because those initiating the regulation do not generally have to pay for it but are simply forcing industry to do so. Collectively, we must maintain our guard against such a potential development.

As part of that process, a new maritime industry consultative Forum has been established to facilitate industry/Government consultation regarding high level policy,

operational, legal and other relevant issues with the view to reaching agreement on practical and cost effective solutions; thus assisting the Office of Transport Security in its role of national maritime security regulator. Hopefully, it will avoid the potential detrimental approach of over regulation.

There are nevertheless serious concerns within industry that as time goes by there is a serious increasing impact on business of the costs of security. The MSICs are a case in point, with each card costing say on average $180 which, if 130,000 are issued, would cost industry $23 million in its first year of implementation with an ongoing cost of say a quarter of that amount.

Ports in many countries have sought to pass on the cost of security, in particular Europe and the United States. In Australia, Brisbane, Sydney, Melbourne, Adelaide and Fremantle have increased wharfage charges, generally being a charge on cargo to recover their own increase in security costs of an average of around AU$2 per container. Additional, ships agents are forced to accept greater and wider responsibilities and liabilities as a consequence of these charges and, of course, incur added expenses in order to comply.

The major stevedores in Australia have also applied different levies in the range of AU$4.50 to AU$4.90 to cover their own increased security costs, primarily from the beginning of 2005. In addition, a number of shipping lines have announced global charges to cover their ship based costs following implementation of the ISPS Code which includes each ship having a ship security plan, Ship Security Officer, a Company Security Officer along with a requirements for the IMO ship number to be clearly displayed on vessels, a ship alert system, an Automatic Identification System (AIS) for short range tracking and so on. These costs have ranged from US$6 to US$10 per container.

There is value, in may view, in these charges being separately identified and kept transparent so that they can be monitored closely and also act as a break on the tenancy to introduce new regulations that could well have limited effect in terms of preventative measures but could be quite costly. We need to avoid the hidden charges for example access cards and their cost to shipping agents as it should be born, in mind that the MSIC card is not designed as an access card but rather to help ensure those that are issued with such cards have been subject to certain identity checks. In other words, the costs of these access cards can be quite high for individual shipping agents and such costs are not readily transparent.

Potentially there are significant benefits for exporters and importers arising from reduced theft and loss, containers being subject to lower levels of inspection and reduced administrative costs as a result of the greater use of electronic documentation by adopting increased security measures.

Cargo theft is a US$350 billion a year business and over 50% is caused through pilferage by people who are at the right place at the right time. Increased security of the container itself, more accurate documentation and a greater degree of alertness will significantly reduce this huge cost impost on world trade.

Conclusion

I have been discussing so far, the preventative measures that have been introduced in Australia but I stress that each and every business does need to develop their own security measures and importantly develop business continuity plans should there be a terrorist attack or other catastrophes that may befall an individual business.

The major test will be if we move to IMO risk level 2 (high) or level 3 (extreme) and in that respect we need the resources to meet that challenge. A high level of coordination and seamless inter-agency response will be essential if a contingency arises and realistic exercises are most important as well as the auditing of security plans if we are to achieve that objective.

One of the greatest risks to our protection against a terrorist attack could well be increasing complacency as time goes by.

Thank-you.

End