THE ASSOCIATION OF AUSTRALIAN PORTS AND MARINE AUTHORITIES INCORPORATED

Level 16, 1 York Street, Sydney NSW 2000
PO Box N590, Grosvenor Place, Sydney NSW 1220
Tel: (02) 9247 7581 Fax: (02) 9247 7585
Email: aapma@aapma.org.au
ABN: 35 182 209 946

11 July 2005

Ms Maureen Weeks
Committee Secretary
Senate Rural and Regional Affairs
and Transport Legislation Committee
SG62, Parliament House
CANBERRA ACT 2600

Dear Ms Weeks,

Inquiry into the Administration of the *Maritime Transport and Offshore Facilities Security Amendment Bill 2005*

We are pleased to respond to the invitation to make a submission to the Committee's inquiry into the Maritime Transport and Offshore Facilities Security Amendment Bill 2005.

The Association of Australian Ports and Marine Authorities
The Association of Australian Ports and Marine Authorities (AAPMA) is the peak body representing the interests of government owned and privately owned ports as well as marine regulatory authorities in Australia. The Association provides leadership and support in areas of common interest related to ports, their interfaces and the achievement of their trade facilitation objectives. A list of our members is included at Appendix I.

Australian ports have welcomed the new maritime security environment and worked closely with DOTARS on the implementation of every aspect of the Maritime Transport and Offshore Facilities Security Act for many months prior to its introduction on 1 July 2004. Maritime Security Identification Cards are an important and integral part of this new maritime security environment.

Maritime Security Identification Cards ("MSICs")
DOTARS held an initial seminar to discuss MSICs in September 2004 to which a broad range of representatives from the maritime industry were invited. A smaller Working Group was formed and first met in October 2004. To date, this Working Group has met regularly, under the chairmanship of DOTARS, and with a fairly consistent membership. The Group has established an excellent working relationship with a high level of trust operating. Indeed, DOTARS is to be complimented on its level of engagement with industry and the unions throughout the MSIC process.

Both the members of the industry Working Group and DOTARS have recognised, from the outset, that MSICs would be implemented into a completely different working environment from ASICs. For instance it is not intended, at this stage, that the entire port population would require an MSIC (unlike most of those working in airports).

The list of crimes against which background checks will be carried out by the AFP and ASIO is different from those applicable to ASICs. The MSIC list focuses on crimes against terrorism and include crimes involving a bomb threat, espionage (and other offences against Part 5 of the *Criminal Code*), involvement in the sale of a weapon of mass destruction, inciting mutiny, hijacking, endangering the security of ports, money laundering and other crimes associated with organized crime or racketeering, people smuggling, crimes involving counterfeiting or falsification of identity documents.

<u>Background Checks and the Application of Common Standards</u>
The AFP and ASIO will undertake criminal background checking of current employees. The background checking process may highlight people against whom an "orange flag" may be raised during the background checking process. It has been recognised by all members of the Working Group and DOTARS that some level of discretion must be applied to certain offences if highlighted during this background checking process.

In the Aviation environment, the Issuing Body assesses anyone against whom an "orange flag" has been raised. We are aware, from a number of sources, that consistency has not been applied to this discretionary process given the number and range of aviation Issuing Bodies. The MSIC Working Group argued, and DOTARS has agreed, that DOTARS will be the determining body during the initial roll-out of MSICs from 1 October 2005 to 30 June 2006.

However, it is the unanimous view of all of the members of the Working Group that an independent Government assessor must continue this determination post 1 July 2006. Delegating this role back to MSIC Issuing Bodies will give rise to inconsistency of application of policy relating to accepting or disqualifying "orange flagged" applicants. It will also give rise to "forum shopping" by applicants for MSICs. We can see a situation arising in which an applicant is refused an MSIC by one Issuing Body only to go elsewhere in the country (perhaps to a regional area where his or her skills and qualifications are urgently required) and obtain an MSIC. Delegating this role to an

Issuing Body would involve a transfer of risk that is surely unacceptable to the Government.

The model drawn up by the Working Group embraces a high level of confidentiality for the MSIC applicant. For reasons of privacy, Issuing Bodies do not want to know any of the detail of the crimes listed on an applicant's MSIC consent form. A number of Maritime Industry Participants, who foreshadowed a willingness to take on the role of an Issuing Body, have indicated that they would not do so if they were exposed to knowledge of an applicant's criminal past, and also forced to be the determining body for "orange flagged" applicants.

Following representations made by members of the Working Group, DOTARS will undertake a review of its role during the implementation process. We understand that there are financial implications with DOTARS, or any other government agency, assuming this role and these are therefore policy questions which the Government must address. As mentioned earlier, the Working Group unanimously believes that the role accepted by DOTARS as determining body during the rollout phase must be an ongoing responsibility of Government.

Need for Ongoing Criminal Database Management

We have been urging the AFP representatives who attend Working Group meetings that the AFP should liaise with the state police forces and co-ordinate their respective databases to ensure that criminal background checks can be live and ongoing rather than the present system whereby they must be updated at the end of the life of the relevant identity card (five years for MSICs). ASIO checks are live and ongoing thus providing continuity to the security aspect of the background checking process.

We understand that the AFP and the state police forces are talking to one another but it is unfortunate that it appears that continuous checking may not be possible for a number of years yet. This is a major weakness and does not appear to meet the security standards that the Government is setting.

Improvements in security are event-driven. The need for continuous police checks is an obvious one and should not require a security event for the process to be fast-tracked.

Potential Industrial Relations Impact

Applicants who are refused an MSIC by a Government body will have avenues of appeal through the AAT. This is presently not afforded to refused ASIC applicants who are assessed by aviation Issuing Bodies. There is, however, also a likelihood of industrial disputation and exposure of employers to unfair dismissal litigation brought by current employees who have been refused an MSIC (and consequently displaced from their employment). These industrial relations implications reinforce the necessity for the approval agency to be seen to be independent of the Issuing Body (who may also be the employer). This has been raised with DOTARS at meetings of the MSIC Working Group.

Government Security Vetting Agency

Minister Anderson's announcement on 7 June 2005 advised that the Government has asked for advice on the establishment of a security-vetting agency. We would support the establishment of such an agency, perhaps set up under the umbrella of the Attorney-General's Department, which could become the determining body for MSICs (as well as ASICs and the identity cards that will be introduced to cover the handling and transportation of ammonium nitrate and other security sensitive goods). Such a body should also manage a national database of MSIC holders that would provide current information on the holder, including their photograph.

Responding to Emergency Situations

The Regulations presently permit (Reg. 6.07N) access to a maritime security zone by ambulance, rescue or fire service officers who are responding to an emergency. The Working Group has noted that this provision does not cover situations such as oil spills or marine incursions. When there is an oil or chemical spill, the usual custom is to establish teams of people from a range of organisations to respond to the spill and its side effects, as well as to engage in response-learning experience. It becomes a multi-jurisdictional activity with environment agencies, local councils and community groups involved. The emergency resulting from the Lara D'Amato spill in Gore Bay, Port Jackson several years ago, lasted for several days and involved a whole range of emergency responders.

We have been advised by DOTARS that the re-wording of the relevant sections requires legal advice with likely policy implications and we understand that work is progressing on this front. Ports are seeking Regulations that will permit both the requirements for MSICs and relevant requirements of the port security plan to be suspended for the duration of the emergency.

We note that care must be exercised as to how access to maritime security zones will be managed by the port for this broader range of emergency responders. We are asking that consideration be given to using the Secretary's exemption power as outlined in these Regulations, on the clear understanding that a post-event notification to the Secretary would take place. This is a very important issue and we are awaiting DOTARS' advice with considerable interest.

Tamper Evident Feature

The card itself will need to carry a tamper evident feature. We have been aware of this requirement from the inception of the consultation process and we have pointed out to DOTARS failings with the tamper evident feature (the "kinegram") applied to ASICs. However, it was not until the Working Group meeting held on 28 June 2005 that we had a presentation on the alternative tamper evident features that are available on the world market. No decision has yet been made by DOTARS and 1 October is rapidly approaching. Those Issuing Bodies who will also choose to manufacture the cards will need to invest in the appropriate machinery, provide training to staff, etc. This part of the process has not been managed in the most efficient manner.

Terms of Reference

(a) Privacy

The question of whether the regulatory framework to be implemented adequately protects privacy interests is entirely dependent upon the Issuing Bodies not having access to background checking information (ie AFP and ASIO checks), as is the current practice in the aviation sector. The privacy of applicants will not be appropriately protected if DOTARS or a Government security-vetting agency were not to remain responsible for the co-ordination and adjudication role after 1 July 2006 and for the life of the MSIC legislation.

(b) Cost Recovery Model

We believe that the cost recovery model is appropriate as the Regulations permit Issuing Bodies to recover their costs.

(c) *Law Enforcement Mechanisms*

Members have established and now maintain contact with their respective police forces through local area commands, marine area commands (if applicable) and the counter-terrorism command, each of whom may be a member of the port security committee. In the majority of cases (and where resources permit), the response when required has been commendable. However, where police capability is less than what is required to meet port security needs, there will have to be additional maritime security law enforcement mechanisms. Any increase in law enforcement mechanisms would be in the public good and therefore should attract appropriate State Government funding. There also has to be a greater liaison between DOTARS and the respective state police forces to ensure that the police are aware of the offences under the Maritime Transport and Offshore Facilities Security Act and prosecute offenders with the full force of the relevant and available law.

(d) Oversight and Compliance Inspection Mechanisms

Oversight and compliance inspection mechanisms for MSICs will be the responsibility of DOTARS' Maritime Security Inspectors and law enforcement officers (AFP, state police and Customs). However, we question the lack of Maritime Security Inspectors presently employed by DOTARS as being insufficient for the task. We are not aware of any consultations between DOTARS and the various law enforcement agencies to determine what impact any compliance activities may have on respective agency operations. We believe that there is an ongoing consultative role for the MSIC Working Group in discussing this and other issues as the cards are rolled out.

(e) Security Checks for Foreign Seafarers

With regard to the adequacy of existing security checks for foreign seafarers, we note that Customs receives a full crew listing 48 hours prior to the ship's arrival. Customs then checks all crew members by name through a database which is linked to other agencies. Crew members of interest are "red flagged" and appropriate action taken. This information, combined with intelligence and ship and cargo risk assessment procedures, are used to provide a border control risk or threat level for the vessel. OTS is privy to this information and can react accordingly through the issue of specific security directions to ports, if required.

However, when foreign crews are leaving the ship for shore leave, there appears to be a wide range of security checks, depending on the practice of the port or the particular facility. We are also aware that there has been equal confusion on the part of visiting foreign seafarers due to their lack of understanding of what is required of them by the facility or the port.

Visiting foreign seafarers are required to carry photographic identification with them when they are going ashore and returning to the ship. Some facilities seek to ease the access to shore by issuing temporary access cards, which do not carry personal photographs, and we have heard that such systems can be abused (the photo identification does not mean that the seafarer has been through security background checking).

This highlights the fact that there incomparable procedures between facilities and that a lack of consistency is being applied by DOTARS in the application of the policy between different facilities and ports. We are ensuring the security of Australian seafarers through the issuing of MSICs, however, insufficient attention is being paid to visiting seafarers.

We recognise that the security environment in which we are all now working is an evolving one to which Government and ports alike will need to respond as incidents and the occasion demands.

Yours sincerely,

Susan Blackwell
Executive Officer

Appendix 1 – List of AAPMA Port Corporation Members

- Albany Port Authority
- Broome Port Authority
- Bunbury Port Authority
- Bundaberg Port Authority
- Burnie Port Corporation Pty Ltd
- Cairns Port Authority
- Darwin Port Corporation
- Esperance Port Authority
- Flinders Ports South Australia
- Fremantle Port Authority
- Geraldton Port Authority
- Gladstone Port Authority
- Hobart Ports Corporation Pty Ltd
- King Island Port Corporation Pty Ltd
- Mackay Port Authority
- Melbourne Port Corporation
- Newcastle Port Corporation
- NSW Waterways
- Port Hedland Port Authority
- Port Kembla Port Corporation
- Port of Brisbane Corporation
- Port of Devonport Corporation Pty Ltd
- Port of Launceston Pty Ltd
- Port of Portland Pty Ltd
- Ports Corporation of Queensland
- Rockhampton Port Authority
- Sydney Ports Corporation
- Toll Ports and Resources - A Division of Toll Logistics
- Townsville Port Authority