

Maureen Weeks
Committee Secretary
Australian Senate Rural and Regional Affairs and Transport
References Committee and Legislation Committee
Parliament House
CANBERRA ACT 2600

**Subject: Submission to the Committee's inquiry into the *Maritime Transport Security
Amendment Act 2005***

Dear Ms Weeks

On 12 July 2005 the Department of Transport and Regional Services attended the public hearing of the Committee concerning the inquiry into the *Maritime Transport Security Amendment Act 2005*. A number of issues were raised by the Committee and the public which we believe required further clarification.

Enclosed for the Committee is DOTARS submission, providing a statement against the Committees Terms of Reference and responses to questions and requests for additional information as requested by the Committee relating Maritime Security Identification Card particularly, s15HB and Part II of the Crimes Act 1914.

Attachment A - Statement against the Terms of Reference of the Committee

Attachment B - Summary of Questions on Notice

Attachment C – Responses to Questions on Notice

If the Committee wishes to discuss any of the information provided in this submission I can be contacted in telephone 6274 6796.

Yours sincerely,

Ross Hallinan
Acting General Manager
Maritime Security Branch

SENATE
RURAL AND REGIONAL AFFAIRS TRANSPORT LEGISLATION COMMITTEE
Tuesday 12 July 2005

To inquire into and report on:

The regulatory framework being implemented and enforced by the Department of Transport and Regional Services under *the Maritime Transport Security Amendment Act 2005*, having regard to

- a) Whether the regulatory framework to be implemented adequately protects privacy issues;
- b) The appropriateness of the cost recovery model in respect to such an important area of national security;
- c) The adequacy of law enforcement mechanisms available to enforce the regulatory scheme;
- d) The adequacy of oversight and compliance inspection mechanisms;
- e) The adequacy of existing security checks for foreign seafarers;
- f) The fair operation of security checks with respect to existing employees; and
- g) The adequacy of consultation mechanisms in respect to the regulatory framework.

Overview - Maritime Security Identification Card

As part of strengthening Australia's maritime security, the Government announced on 20 July 2004 the introduction of the Maritime Security Identification Card (MSIC). On 15 December 2004, the Prime Minister extended the Maritime Transport Security Act 2003 to offshore oil and gas sector, which effectively extended the scope of the MSIC to offshore oil and gas facilities.

The MSIC is a nationally consistent identification card that identifies the holder as having met the background checking requirements to be in a maritime security zone. All persons requiring unmonitored access to a maritime security zone including offshore security zones will require an MSIC. Those persons requiring unmonitored access could include, port and port facility workers, seafarers, transport operators and offshore oil and gas workers.

The MSIC will not be an access control card existing access arrangements as approved in Maritime Security Plans will continue to operate. However, if a Maritime Industry Participant wishes to, they may incorporate an access control onto the MSIC. The incorporated access control features will not be regulated.

It has been proposed that background checking for the MSIC will commence from 1 October 2005. Due to the anticipated large number of potential MSIC holders the rollout will span 9 months. From 1 July 2006 all unmonitored persons in a maritime security zone will be required to hold and display an MSIC.

MSIC will be issued by an issuing body which could be maritime industry participants, employee or employer associations and any other organisation authorised by the Department of Transport and Regional Services.

The prospective MSIC holder will need to consent to a criminal history check to be undertaken by the Australian Federal Police (AFP). The AFP consent form will also ask the applicant to acknowledge that a check by the Australian Security Intelligence Organisation (ASIO) will be undertaken.

In the implementation phase DOTARS will manage the process of making decision on the basis of the criminal history check by the AFP and ASIO and will inform the issuing body and the applicant if they are or are not eligible to hold an MSIC. During the implementation phase DOTARS has also committed to review its ongoing role in the post implementation phase.

MSICs will only be issued to those persons who have successfully met the background checking requirements. If a person is not eligible for an MSIC it will become a matter for the employer and employee to negotiate alternative working arrangements.

a) Whether the regulatory framework to be implemented adequately protects privacy interests

Under the MSIC Scheme applicants will be protected by the *Privacy Act 1988*. The Privacy Act states that all personal information must only be used in accordance with the National Privacy Principles. The National Privacy Principles sets out the standards for the collection, use, disclosure, quality and security of personal information. All information disclosed on an applicant must be done so within the meaning of the Privacy Act.

The Privacy Act states that the information collected must only be used for the purpose it was collected. As personal information will only be collected for the purpose of issuing an MSIC it would be illegal for an organisation to use this information for any other purpose.

During the implementation phase 1 October 2005 until 30 June 2006 DOTARS will determine if a person has an adverse criminal record, based on the results of a criminal history check conducted by the AFP and a security assessment conducted by ASIO. Industry will not receive any personal information on their employees. They will however, receive advice from DOTARS on whether they can or can't issue an MSIC.

During the implementation phase DOTARS has agreed to review its ongoing role. If this function was to be undertaken by the maritime industry they would be obliged to act within the privacy act.

b) The appropriateness of the cost recovery model in respect to such an important area of national security

Consistent with the Australian Government's policy that security is a cost of doing business, industry will be responsible for the implementation and cost of introducing the MISC Scheme.

Provisions under the Maritime Transport and Offshore Facilities Security Regulations 2005 allow for all reasonable costs incurred by a person involved with issuing an MSIC to be recovered from the person who requested the MSIC.

Each MSIC issuing body will determine how they recover their costs associated with the issuing of an MSIC. Based on previous experience with the aviation industry, it is anticipated that some MSIC issuing bodies will cover the cost of issuing an MSIC for their direct employees and charge all other MSIC applicants.

Based on the average costs currently incurred by the Aviation Industry for the issuing of an Aviation Security Identification Card (ASIC) it is anticipated that an MSIC will cost approximately \$150, which includes the cost of the AFP and ASIO checks. The MSIC is valid for five years which equates to an annual cost of approximately \$30 a year.

In regard to the introduction of the MSIC Scheme, DOTARS will incur administrative costs for the regulation of the MSIC Scheme. Funding of \$1.9 million was allocated by Government in 2003-2004 over four years to introduce the MSIC Scheme for the implementation of the MSIC Scheme and to provide ongoing policy advice to the maritime industry.

c) The adequacy of law enforcement mechanisms available to enforce the regulatory scheme

To assist maritime industry participants to secure their maritime security zone, offence provisions have been set out in the *Maritime Transport and Offshore Facilities Security Act 2003* and *Maritime Security and Offshore Facilities Security Regulations 2005*.

For example, there is an offence to ban unauthorised persons from entering a facility.

As from 1 July 2006 those persons who are not displaying an MSIC or being escorted or continuously monitored by an MSIC holder will not be authorised to be within a maritime security zone.

Section 151 of the Act defines 'law enforcement officers' who are able to exercise powers under the Act. Law enforcement officers are members of the Australian Federal Police, the police force of a State or Territory, and customs officers prescribed in the regulations.

Sections 153, 154 and 155 of the Act provide that a law enforcement officer may stop and search any person, vehicle or vessel within a maritime security zone or on-board a security regulated ship.

In addition to enforcement by the police force of a State or Territory and members of the Australian Federal Police, Maritime Industry Participants must, in their security plans, set out security measures and procedures to monitor and control access to the security zone, including measures to detect and deter unauthorised access to the zone.

d) The adequacy of oversight and compliance inspection mechanisms

During the implementation phase from 1 October 2005 until 1 July 2006, DOTARS will determine if an MSIC applicant is eligible to hold an MSIC based on the outcome of the AFP criminal history check and ASIO security assessment. DOTARS will also assess MSIC plans, and liaise with industry.

Post implementation DOTARS will undertake audit and compliance activities for MSIC Scheme. Where the regulations are not being adhered to, persons or organisations will receive a warning, an infringement notice or a penalty.

DOTARS' ongoing regulatory roles and responsibilities will include:

- assessment of MSIC Plans;
- audit of MSIC Plans;
- checking compliance;
- regular liaison with other Commonwealth departments and State and Northern Territory authorities; and
- Policy advice and guidance to industry.

Maritime industry participants must demonstrate that they meet security requirements to lawfully operate. The Department has responsibility for monitoring and ensuring the compliance of maritime industry participants in regard to the act and regulations. It is appropriate for the Government to explicitly regulate in this area.

While the consequences of a terrorist incident are catastrophic, market forces cannot be relied upon to arrive at the optimal level of security. In addition to this fact, the ownership arrangements within the

maritime industry means that it would be impossible to guarantee consistency in the absence of Government enforced standards.

e) The adequacy of existing security checks for foreign seafarers

Seafarers employed on an Australian regulated ship, regardless of their nationality, will be required to hold a MSIC. Foreign seafarers on Australian regulated ships will be required to undergo the same background checking process as an Australian seafarer. They will need to have ASIO and AFP checks conducted on them, and will need to provide proof of their eligibility to work in Australia.

The MSIC Scheme can not apply to foreign seafarers on foreign flagged ships, this is the responsibility of contracting governments as set out in the International Ship and Port Facility Security Code. Foreign seafarers on foreign ships will need to be escorted or continuously monitored while they are in an Australian regulated maritime security zone.

f) The fair operation of security checks with respect to existing employees

All employees both new and existing will undergo the same background checks. If a person is found to be ineligible to hold an MSIC they will not be allowed to enter or remain in a maritime security zone.

In the event of an applicant not being able to obtain a MSIC, they will have access to appeal mechanisms through the Secretary of the Department of Transport and Regional Services and the Administrative Appeals Tribunal.

g) The adequacy of consultation mechanisms in respect to the regulatory framework

In developing the MSIC administrative framework DOTARS has undertaken consultation with the Maritime industry.

Initial meetings in July 2004 and August 2004 were conducted with a range of maritime industry participants to identify an appropriate consultative forum for the MSIC initiative.

Maritime industry participants, peak industry bodies and employee representative groups were invited to attend a two day workshop in Sydney on 27 and 28 September 2004 to discuss issues associated with the implementation of the MSIC initiative.

The MSIC Working Group was established as a result of nominations by industry at the September 2004 workshop. It was established to assist in the development of the regulatory and administrative framework for the delivery of the MSIC scheme. The MSIC Working Group is made up of representatives from:

- Department of Transport and Regional Services
- Australian Federal Police
- Australian Security Intelligence Organisation
- Australian Customs Service
- Australian Maritime Safety Authority
- State Governments
- Port Operators
- Port Facility Operators

- Port Service Providers
- Ship Operators
- Peak Industry Bodies
- Employee representatives
- Supply Chain stakeholders

The MSIC Working Group has met regularly to discuss issues associated with the design of the MSIC regulatory architecture and to be kept informed on key issues affecting the implementation of the MSIC scheme.

DOTARS acknowledges the important involvement and dedication of the Working Group in assisting in the development of the MSIC Scheme. Consultation has taken the form of both face to face meetings and electronic and telephone communication.

With the Government's announcement in December 2004 that the offshore oil and gas industry would be bought under the coverage of the *Maritime Transport Security Act 2003* the scope of those persons affected by the introduction of the MSIC Scheme was wider.

To ensure that the offshore oil and gas industry were consulted on the introduction of the MSIC Scheme officers from the Department of Transport and Regional Services visited offshore oil and gas operators and the Australian Petroleum Production and Exploration Association between 10-12 May 2005.

Due to the Government's timeframe for the implementation of the MSIC Scheme the Working Group met on 28 June 2005. At this meeting members were advised that the next set of draft regulations to be circulated would be presented to the Executive Council on 21 July 2005. They were also advised that any issues raised by the working group during that meeting that could be amended in the draft regulations without further policy considerations would be reflected in the next set of draft regulations circulated to the working group.

Details of those issues raised by the Working Group which could not be included in the draft regulations as they required additional policy approval or were beyond the scope of the MSIC Scheme were circulated to the Working Group on 29 June 2005. DOTARS gave a commitment to follow-up on these issues and to also proceed with the making of the MSIC regulations to give industry certainty.

At the Senate Committee inquiry members of the Working Group expressed concern that the draft set of regulations circulated on the 8 July 2005 (attachment A1) differed dramatically from the previously circulated version of 27 June 2005 (Attachment A2). DOTARS would like to advise the Committee that this was not the case. The version of the regulations circulated on 8 July had been settled by the Office of Legislative Drafting and Publishing which had resulted in some minor corrections of drafting errors, renumbering and minor reordering of some regulations. The final set of regulations did not diverge from the policy principles that had been agreed to by the Working Group.

Hansard- Senate Committee Meeting 12 July 05- Questions taken on Notice and other issues

Question Number	Subject	Summary of Senate Committee Transcript	Page number and reference
1	Table of disqualifying factors	ACTING CHAIR (Senator Ferris)—I think you offered to Senator Heffernan before he left that you would put a paper to us which might clarify that list of disqualifying factors and give us some context for them. It would be very useful if the committee could have that. Mr Tongue—Certainly.	Mid Page 63
2	Understanding of the crimes list	Senator FERRIS—But there are some confusing items, Senator O'Brien. Senator O'BRIEN—I am saying that there may be some where you would argue as to whether they should be disqualifying or exclusionary. Senator FERRIS—If hijacking an aircraft is an exclusion but harming Australians is a disqualification, what does it say to the pilot? Surely the hijacking of an aircraft— CHAIR—Do not have any Australians on it. Senator FERRIS—When you do the paper for us, Mr Tongue, these are the sorts of things that I need to better understand. An aircraft is being piloted or a ship is being captained and that person is presumably an Australian; I would have thought that they were harmed by a hijacking. Therefore, how is it that you can have hijacking in an exclusion area and harming Australians in a disqualifying area? Mr Tongue—It depends on what a person is charged with. A person may commit an offence and be charged with multiple offences. CHAIR—These are not charges; these are criminal convictions. Mr Tongue—They may be convicted under multiple parts of— Senator FERRIS—Can you explain that in the paper you send to us? That confuses me; I would have thought that that pilot was potentially being harmed. Mr Tongue—Okay.	Starts middle of page 66, Question from Senator Ferris
3	Definition of Damage to Commonwealth property	Senator WEBBER—With your indulgence, Chair, I have a couple more issues I would like to explore. Before I do that, Mr Tongue, you undertook to come back to us with a table. Mr Tongue—Yes. Senator WEBBER—Within that table, can you give me a definition of what serious damage to Commonwealth property is? Mr Tongue—We will do our best, talking to lawyers—	Starts Bottom of Page 72 Question from Senator Webber
4	Notification to working group of 15HB being a mistake	Senator WEBBER—Did you tell them that it was not meant to be 15HB, it was meant to be part II, and that that was a drafting mistake? It seems to me that if you had, it would have prevented a whole lot of angst. Ms Liubestic—I certainly recall there was mention of it. But it was a very long meeting. Senator WEBBER—So they were told? Ms Liubestic—My understanding is that they were. Senator WEBBER—Were you there? Ms Liubestic—Yes, I was. Mr Tongue—Can we go back and check the minutes of the meeting? Senator WEBBER—That would be useful. This is a significant change. If they were not told that there was a drafting mistake in the earlier regulations that you were having your	Top of Page 72, Question from Senator Webber

		extensive consultations around—and we were coming up with an agreed consensus document around—we have a fundamental problem.	
5	15HB a mistake	<p>Senator O'BRIEN—But 15HB is entitled 'What is a serious Commonwealth offence or a serious State offence that has a federal aspect?' Are you saying that that was in there by mistake? It says:(1) For the purposes of this Part, serious Commonwealth offence means an offence against a law of the Commonwealth: (a) that involves theft, fraud, tax evasion, currency violations, illegal drug dealings, illegal gambling, obtaining financial benefit by vice engaged in by others, extortion, money laundering, perverting the course of justice, bribery or corruption of, or by, an officer of the Commonwealth, an officer of a State or an officer of a Territory, bankruptcy and company violations, harbouring of criminals, forgery including forging of passports, armament dealings, illegal importation or exportation of fauna into or out of Australia, espionage, sabotage or threats to national security, misuse of a computer or electronic communications, people smuggling, slavery, piracy, the organisation, financing or perpetration of sexual servitude that is punishable on conviction by imprisonment for a period of 3 years or more.</p> <p>Ms Liubestic—Could I take this on notice? Obviously, there have been various versions of the regulations sent out. I am looking at the most current version, which does not have that issue listed.</p>	Middle Page 71 Question from Senator O'Brien
6	Transport Security Inspectors	<p>"How many of those [staff in the state offices who are transport security inspectors], in the state offices, would regularly visit these workplaces as well as do their other duties?"</p>	Top of Page 62, Question from Senator O'Brien
7	Exemptions from secretary for displaying, holding or carrying an MSIC.	<p>Senator O'BRIEN—Draft regulation 6.07M provides for the secretary of the Department of Transport and Regional Services to exempt certain persons or classes of persons from holding, carrying or displaying an MSIC. This is not a reg that concerns the defence forces or emergency services personnel that are dealt with in 607J2(b) and 6.07N. What persons or classes of persons will be eligible to receive this exemption?</p> <p>Ms Liubestic—The exemption is if there is an occupational health and safety issue with the wearing of the MSIC in a particular zone. So if you have an MSIC dangling on the end of a lanyard which could get caught on machinery, that is what that clause is referring to.</p> <p>Senator O'BRIEN—So it is not, as someone has suggested, about getting people in to deal with an oil spill or something.</p> <p>Ms Liubestic—The MTSA Act is about allowing those people dealing with those emergencies to come into the zones and to deal with the emergencies where they do not have to have the requirement of displaying the MSIC.</p> <p>Senator O'BRIEN—So that is covered under the act.</p> <p>Ms Liubestic—That is right.</p> <p>Senator O'BRIEN—If there are occupational health and safety circumstances where the wearing of the card will be the subject of consideration for exemption, is that defeating the purpose of the card?</p> <p>Ms Liubestic—It is an exemption from being displayed rather than actually holding the card. You would still have to go through all the background checking processes so you would still have the card. We would envisage some circumstances, such as in the offshore oil and gas situation where you are working around machinery, where the card dangling around your neck may cause a problem in terms of occupational health and safety, but you would still</p>	Mid Page 62, Discussion between Patricia L and Senator O'Brien

		have to go through the process of obtaining the card	
8	Disqualifying notice, and access to MSZ	<p>Senator O'BRIEN—Again, 6.07K(1) provides that a person who has been given a disqualifying notice must not enter a secure area. It can be issued to a person who has been convicted of an offence listed in items 1 or 2 of the table in 6.07C, including treason, espionage and supplying weapons of mass destruction. Draft regulation 6.07K(2) provides a significant exemption, I would suggest, to this prohibition on entry for a person convicted of a disqualifying offence who is:</p> <p>... a visitor to a zone for the purpose of boarding or leaving a vessel as part of a recreational activity.</p> <p>Why should those persons be exempted for that purpose and thus be able to, unescorted, potentially enter a secure maritime zone?</p> <p>Ms Liubestic—I do not think it actually says that. I think it means that somebody who has been convicted of those particular crimes actually needs to be escorted.</p> <p>Senator O'BRIEN—I am sorry; where does it say that?</p> <p>Mr Tongue—Can we come back to you on that one?</p> <p>Senator O'BRIEN—You certainly can. I make the point that there does not appear to be anything that I can see in the regulations that would require—</p> <p>Mr Tongue—The intention is the reverse. We will have to check with our drafters.</p>	Bottom of Page 62, Top of Page 63, Question from Senator O'Brien
9	Breakdown of Costs	“Can the committee be provided with a breakdown of costs associated with the introduction of the MSIC, and the extension of the maritime security regime to offshore facilities?”	Bottom of Page 63, Question from Senator O'Brien
10	Abuse of the Maritime security regime	“The committee heard evidence that a small number of industry participants have abused the maritime security regime to achieve other objectives, including preventing representatives of the International Transport Workers Federation from communicating with ships crews. In May Mr Kilner told the committee that the department had investigated two complaints related to this issue. What was the outcome of those investigations?”	Bottom of Page 63, Top of 64, Question from Senator O'Brien
11	Administration of the costal shipping permit system	“Can you advise the committee of whether or not any deficiency in the administration of the costal shipping permit system has been identified by any internal or external audit?”	Bottom of page 66, Question from Senator O'Brien
12	Foreign Seafarers	<p>Senator O'BRIEN—Do we know how many foreign seafarers enter Australian ports each year?</p> <p>Mr Tongue—In excess of 200,000.</p> <p>Senator O'BRIEN—Do we know how many of those crew are from flag of convenience vessels?</p> <p>Mr Tongue—No. I have to take that one on notice.</p>	Top of page 67 Question from Senator O'Brien

<p>13</p>	<p>Container security</p>	<p>Senator O'BRIEN—One of the issues raised in the joint union submission to this inquiry, and identified as a security gap in the ASPI report, is poor container security. We are told that no empty containers are screened, but how many empty containers are brought through Australian ports each year? Mr Tongue—We tend to deal with Customs on that one. I would be chancing my arm on empty containers. Can I take that one on notice? Senator O'BRIEN—Yes. We are told, and perhaps you can confirm, that the number screened is zero. Mr Tongue—I will have to take that on notice.</p>	<p>Starts Bottom of Page 67 Question from Senator O'Brien</p>
<p>14</p>	<p>Commitment to allow WG to quickly comment on the draft regulations</p>	<p>Senator STERLE—And that is not the argument. It leads me to ask you this question: will DOTARS give an undertaking to let the members of the working group have a further opportunity to comment quickly on the latest draft regulations? Mr Tongue—Senator, I think we face a timing problem. We can get them out and try to get comment back quickly, but we would need the indulgence of the industry. It would be a lightning sort of a process, but we will do our best. We will do our best to have a look at timings and see if we cannot get them out again. Senator STERLE—And you will come back to us on this? Mr Tongue—I will.</p>	<p>Bottom of Page 72, Question from Senator Sterle</p>
<p>15</p>	<p>Checking of nature of cargo</p>	<p>Senator WEBBER—so that they can go and buy their beads and bangles, as Senator Heffernan was referring to earlier. What regime do we have in place to check for the transport of, say, things like ammonium nitrate by foreign flagged ships with foreign crews? Do we have a security arrangement for that? It could potentially go around Australia. Mr Tongue—One of the things that occurs if, say, ammonium nitrate is being carried on a single voyage permit or a continuing voyage permit, is that we get information on the nature of the cargo when the cargo is being carried. We have some information on what is in those vessels. Senator WEBBER—Is that information that they willingly give you? Mr Tongue—No, that is part of the process of going for a continuing voyage permit or a single voyage permit. That is part of the process. Senator WEBBER—How do you find out? We have heard how only a very small number of containers are screened, so how do you know? Mr Tongue—Senator, you are going a bit beyond my knowledge there, and I do not have the relevant person with me. Can I provide that on notice?</p>	<p>Top of Page 74, Question from Senator Webber</p>
<p>16</p>	<p>Incorrect information given in hearing regarding monitored access</p>	<p>Senator WEBBER—I have one final issue. Regarding the people who access the maritime security zones and do not have an MSIC, they get escorted around or they can be monitored by closed circuit television? Ms Liubescic—On a continuous basis. Senator WEBBER—Do the people monitoring them on the closed circuit television on a continuous basis have to hold an MSIC? Ms Liubescic—We are looking at the legal advice about that issue. It has been raised with us but quite late in the process.</p>	<p>Middle of Page 75, discussion between PL and Senator Webber</p>

Answers to questions 1, 2 and 3

INTRODUCTION

To be eligible for the issue of Maritime Security Card (MSIC), applicants will need to undergo a series of background checks. These checks will include a criminal history check by the Australian Federal Police (AFP), and a security assessment by the Australian Security Intelligence Organisation (ASIO).

CRIMINAL HISTORY CHECKS

The MSIC Criminal History Check will be undertaken within the protection of the Commonwealth Spent Convictions Scheme. The Commonwealth Spent Conviction Scheme prevents discrimination against individuals on the basis of old minor convictions. Any minor conviction is considered disregarded after a specified period and will not be recorded on a criminal history check.

However, the Department of Transport and Regional Services (DOTARS) has applied for and received agreement from the Privacy Commissioner and the Attorney General's Department for an exclusion from the Spent Convictions Scheme for all maritime-security-relevant-offences.

A criminal history check once completed will result in the issuing of a police records certificate. The police records certificate will include all of the following items:

1. Chapter 5 of the Criminal Code, the security of the Commonwealth which includes treason, espionage or others similar activities, terrorism, harming Australians;
2. involving the supply of weapons of mass destruction;
3. treachery, sabotage, sedition, inciting mutiny, unlawful drilling or destroying or damaging Commonwealth property;
4. interference with aviation, maritime transport infrastructure or an offshore facility;
5. identity offence involving counterfeiting or falsification of identity documents or assuming another individual's identity;
6. transnational crime involving money laundering or another crime associated with organised crime or racketeering;
7. People smuggling and related offences;
8. importing, exporting, supply or production of weapons, explosives or a trafficable quantity of drugs;
9. any conviction with a sentence greater than 30 months;
10. any conviction a person has if they have been repeatedly convicted within a ten year time frame; and
11. any conviction a person has not had excluded from the Spent Convictions Scheme.

All eleven items are included in a police records check however, only items 1 to 8 are defined as Maritime Security Relevant Offences and therefore will be taken into account in determining a person's eligibility for an MSIC.

Under the MSIC Scheme those persons found to have a maritime-security-relevant offence are not eligible to hold an MSIC. Those people found to have a conviction against items 1 and 2 under no circumstances will be considered for the issue of an MSIC.

The Working Group did not believe it was appropriate to automatically disqualify a person from holding an MSIC if they had been convicted of a maritime-security-relevant offence as set out in items 3 to 8, due to the broad way in which offences are described and therefore, the type of actions which would be captured within these items.

For example, a person could be convicted of an identity offence involving counterfeiting or falsification of identity documents or assuming another individual's identity (item 5) if a person:

- a) produced a low tech type of identification such as school identification for the purpose of gaining discount transport; or
- b) manufactured or possessed equipment capable of manufacturing documents relating to citizenship.

For a person convicted for one of these actions their police records certificate will show a conviction for forgery, the date the conviction was recorded and length of conviction.

DEFINITION OF DAMAGE TO COMMONWEALTH PROPERTY

In addition the Committee requested an example of a conviction for Damaging Commonwealth Property; a person could be convicted for damaging Commonwealth Property as mentioned in item 3 for:

- a) graffitiing their initials on a Government building; or
- b) severely damaging a Commonwealth building which has resulted in a great cost to repair.

For a person convicted for one of these actions the police record check will show a conviction for damaging Commonwealth Property, the date the conviction was recorded and the length of the conviction, it will not provide any details of the actions which lead to the conviction.

To allow for the fair and reasonable treatment of all persons applying for an MSIC an MSIC applicant or an issuing body may apply to the Secretary to issue an MSIC to a person who has a conviction against a maritime-security-relevant offence items 3 to 8.

The Secretary in determining if a person may be issued an MSIC will need to take the following into consideration:

1. the nature of the offence the person was convicted of; and
2. the length of term of imprisonment imposed on him or her; and
3. if he or she has served the term, part of the term – how long it is, and his or her conduct and employment history, since he or she did so; and
4. if the whole of the sentence was suspended – how long the sentence is, and his or her conduct and employment history, since the sentence was imposed; and
5. anything else relevant that the Secretary knows about.

EXTENSION OF DISQUALIFYING OFFENCES

Some members of the Senate Committee strongly indicated that some additional crimes on the proposed MSIC list of crimes should be reclassified as disqualifying (no card issued under any circumstances) rather than exclusionary. The Department of Transport and Regional Services (DOTARS) has taken this advice into account. DOTARS is proposing to modify the list of maritime security relevant offences in the regulations to include the hijacking of a ship or aircraft as an automatic disqualifying offence. DOTARS is considering reclassifying some additional serious crimes on the existing list to also become disqualifying.

Answers to questions 4 and 5

Senator O'Brien and Senator Webber asked the Office of Transport Security to clarify the drafting error referenced in regulation 6.07C where there had been a change from 15 HB of the *Crimes Act* 1914 referenced in the first draft of the regulations circulated to the MSIC working group on the 10 June 2006 and the draft circulated to the working group which referenced Part II of the *Crimes Act* 1914 on 8 July 2006.

The answer to the honourable member's question is as follows:

In testimony given by some members of the working group they advised the Senate Committee it was alleged that:

- The Department of Transport and Regional Services (DOTARS) had originally issued a version of the regulations which included a reference to 15 HB of the *Crimes Act* 1914; and
- These members of the working group also advised the Senate Committee that in the most recent version of the regulations DOTARS had later replaced reference 15 HB of the *Crimes Act* 1914 with a reference to Part II of the *Crimes Act* 1914 and that the department failed to provide adequate advice on this change.

The facts are as follows:

- On the 16th of February 2005 the working group met. The agenda and minutes show that exclusionary and disqualifying crimes were discussed (attachments C1&C2). The members of the working group were given a list of the crimes (attachment C3). The list included crimes from Part II of the *Crimes Act* 1914.
- The first draft of the regulations was circulated to the working group on Friday 10 June 2005 (attachments C4 & C5). This version contained an error where a reference to 15 HB of the *Crimes Act* 1914 was incorrectly included.
- This drafting error was picked up and changed in the next version of the regulations which was circulated to the working group on 27 June 2005 prior to the WG meeting on 28 June 2005 (attachments C6 & C7). The correct reference to Part II of the *Crimes Act* 1914 was reinserted. During this working group meeting the regulations were reviewed page by page including the reference to Part II of the *Crimes Act* 1914.
- The regulations were again circulated to the working group again on 8 July 2005 with the reference to Part II of the *Crimes Act* 1914 unchanged from the previously circulated list (see attachment C8& C9).

Thus, 14 days prior to the Senate Committee hearing, all members of the working group had received a version of the regulations that referred to Part II of the *Crimes Act* 1914. Why some members of the working group claim that Part II of the *Crimes Act* 1914 was included into the regulations without any warning is a mystery. Why some members of the working group failed to note the inclusion of Part II of the *Crimes Act* 1914 in the regulations issues on 27 June 2005 is unknown.

MSIC Working Group

Agenda

Date: 16 February 2005

Venue: Port of Melbourne Corporation Board Room, Level 48 Rialto South Tower,
525 Collins St, Melbourne

9.15am Welcome

9.30am Item 1. Government Approach to introduction of the MSIC
(principles discussion)

10.30am Morning Tea

10.45am Item 2. Detailed Discussion on MSIC framework:

- Structure for the delivery of MSIC (scope, issuing bodies, card manufacturing and role of OTS)
- Background checking (exclusion offences and MSIC application form)
- Card technology (biometrics and tamper evident feature)

12.30 pm Other Business

- Next Steps

12.45 Lunch (provided)

Close

MSIC Working Group Meeting Minutes

16 February 2005 – Port of Melbourne Boardroom, Rialto Tower, Melbourne

Attendees:

John Kilner	Office of Transport Security - Canberra
Patricia Liubescic	Office of Transport Security - Canberra
Warwick Bull	Office of Transport Security - Melbourne
Cornelius Pau	Office of Transport Security - Canberra
Tim Killesteyn	Office of Transport Security - Canberra
Leanne Lomas	Australian Federal Police
Peter McCann	Australian Federal Police
Tony Small	Attorney General's Department
Paul Newton	Australian Customs Service
David Baird	Australian Maritime Safety Authority
Mike Williams	Department for Planning and Infrastructure, Western Australia
George Davis	Port of Melbourne
Peter Shepherd	Sydney Ports
Sue Blackwell	Association of Australian Ports and Marine Authorities
Barry Beech	Patrick
Jock O'Hagen	P&O Ports
Wynne Jones	Woodside
Margaret Fulham	Adsteam
Trevor Griffett	Australian Shipowners Association
Stephen Morris	Customs Brokers and Forwarders Council of Australia
Neil Chambers	Victorian Trucking Association
Dean Summers	Maritime Union of Australia
Danni Whyte	Transport Workers Union of Australia
Martin Byrne	Australian Institute of Marine and Power Engineers

Apologies

Llew Russell	Shipping Australia
--------------	--------------------

Meeting notes:

Opening Comments:

- John Kilner opened the meeting and thanked George Davis and the Port of Melbourne for their hospitality in hosting the meeting.
- A brief overview of the meeting was delivered to the Working Group.
- Dean Summers asked whether any information had been presented to the Minister of Transport and Regional Services, the Hon John Anderson MP, to date as the Working Group had not finalised any decisions regarding the MSIC. John Kilner advised that a model developed by OTS had been presented to the Minister but no approval had not been received at that stage.

Government Approach to introduction of the MSIC

- An overview of the principles for delivering the MSIC scheme was delivered. It was stated that:
 1. the MSIC would be a nationally recognised identification to facilitate easy recognition and would apply to persons requiring unescorted access to port security zones, regulated offshore facilities and seafarers onboard Australian flagged ships;
 2. Maritime Industry Participants (MIPs) may choose to incorporate access control onto the obverse side of the MSIC;
 3. unescorted privileges in the above identified areas must only be given to an MSIC bearer however, the MSIC will not grant the bearer access privileges. Access decisions are to be made by facility operators;
 - Sue Blackwell sought clarification on the use of visitor and temporary cards for the MSIC scheme. John Kilner advised that due to abuse of temporary and visitor cards within the ASIC scheme, the MSIC legislation would not regulate these cards. Concerns were raised by Trevor Griffett regarding the logistics of an MSIC bearer having to escort a new employee who could only hold a temporary MSIC as the nature of the industry often requires unescorted access. It was proposed that a subcommittee of the Working Group identify any issues with not implementing a temporary or visitor card, and in conjunction with DOTARS, develop solutions to address these issues.
 4. train and truck drivers requiring unescorted access to Landside Restricted Zones would also require an MSIC;
 5. MIPs that holds an Maritime Security Plan (MSP) can either be MSIC Issuing Body or nominate an entity to act as their Issuing Body;
 - John Kilner clarified that in the aviation industry, major airlines, airports and some government departments act as issuing bodies. It will be a requirement that any organisation wishing to act as an issuing body will need to have an MSIC program approved by OTS before commencing operations. It is anticipated that if less issuing bodies are established, the portability of the card will increase within the industry.
 6. OTS will vet all existing maritime employees that require access to the port security zone;
 - George Davis thanked John Kilner for accepting the responsibility.
 7. OTS will approve any changes that are required to the MSPs with the introduction of the MSIC scheme;
 8. the MSIC scheme will have a rollout period of nine months from 1 October 2005 until 1 July 2006 to assist with the vetting process;
 9. OTS will develop guidance material regarding the development of the MSIC plans and the amendment of MSPs; and
 10. changes to the Maritime Transport Security Act 2003 and Maritime Transport Security Regulations 2003 would be presented to the Australian Parliament in the winter session.
- During the conversation, concerns were raised oil and gas workers had previously been excluded but were now captured in the MSIC scheme.
- Concerns were also raised regarding the glut of MSP applications which was caused during the implementation of the MTSA and that the same problems may occur. However, John Kilner stated that once the legislation had been passed through Parliament,

that applications could be sent to OTS. In the meantime, John Kilner committed to drafting and circulating a draft MSIC plan.

Background Checking:

- John Kilner discussed the application process for the MSICs, and that:
 - applicants would be responsible for submitting their application to the Government for assessment;
 - the issuing body would need to register that the applicant has completed the application, verify the identity of the applicant by way of the 100 point check, and then advise OTS of the applicant's details and individual MSIC number;
 - once the checks have been undertaken by the Government, the application will fall into one of three categories:
 - Green – applicant has been approved to receive an MSIC and will be advised, along with the Issuing Body, of their success;
 - Orange – applicant is not disqualified from receiving an MSIC, however discretion must be exercised relating to the criminal history of the individual. Applications will be reviewed by OTS, the applicant and Issuing Body will be made aware of the result; or
 - Red – the applicant has been denied an MSIC due to information identified within the background checking. The applicant and Issuing Body will be advised;
 - if an adverse politically motivated violence check is established, ASIO will advise the OTS and discuss the issue with the applicant to seek resolution. Less than 1% of applicants in the latest ASIC reissue had their ASICs declined.
- Martin Byrne and Trevor Griffett advised the Working Group that this was not feasible for seafarers and casual employees due to the quick turn around of staff required to fill vacancies on board a ship.
- Leanne Lomas advised the Working Group that it is the employee's responsibility to source overseas criminal history checks as the AFP does not liaise with overseas police departments regarding these matters.
- It was agreed that a sub-committee would be established to discuss the logistics of casual and seafarers issues surrounding MSICs.
- The model which was sent to the Minister by OTS suggested that the re-issue of the MSIC should follow a five year cycle with employees working in the fields of oil and gas and cruise ships undertaking checking every two years.
 - Concerns were raised by Wynne Jones regarding the potential of two different workers, one oil and gas and one port) working 20 metres apart but operating on two different regulatory schemes.
- An applicant leaving the Australian maritime regulatory environment for a period longer than 12 months would trigger a new background check upon re-entry to the environment.
- George Davis advised the group that an individual moving around a shipping container port posed a small risk compared to other ports and queries the role of technology in monitoring the movements in a port security zone i.e. CCTV, direct line of sight.
- John Kilner advised the Working Group that OTS would write to all MSP holders seeking advice on the number of employees that are likely to be affected by the initial rollout of the MSIC.

- Danni Whyte and Dean Summers suggested that the OTS undertake an industry impact statement to determine the potential cost to industry regarding redeployment, redundancies and retraining.
- Margaret Fulham suggested that the Government could establish a structural adjustment package to assist the maritime industry. John Kilner advised that it was highly unlikely that this would occur and no indication of a structural adjustment package had been discussed.

Break for Morning Tea

List of Exclusionary and Disqualifying Crimes:

- John Kilner undertook to have genocide and slavery re-introduced into crimes against humanity.
- Sue Blackwell requested that a guidance paper be developed regarding the ‘orange flag’ crimes and whether an Issuing Body would be able to issue an MSIC if an applicant was captured under these exclusion crimes.
- John Kilner advised that OTS will remain involved in the background checking process past the initial rollout in relation to ‘orange flag’ applicants. OTS’ capacity in this role will be limited to providing policy advice and undertaking reviews of decisions that Issuing Bodies have made if applicants wish to appeal.
- A definitive level was sought regarding the appropriate level of drugs considered to be trafficable. Consensus around the table seemed to indicate that that ‘lowest common denominator’ within State and Territory legislation be used as this figure.

Flowcharts:

- From the outset of the discussions Dean Summers advised the Working Group that it was the MUA’s point of view that the MSIC was a cost of operating within the transport industry and that the cost of the MSIC should not be borne by employees.
- OTS has undertaken to provide a further flowchart regarding the appeal mechanism for the ASIO politically motivated violence check. OTS will liaise with Tony Small to finalise this.

Portability:

- OTS will develop some guidance material regarding conditions on a break in employment triggering a new background check.
- Trevor Griffett advised the Working Group that a break in employment triggering a new background check would severely impact on the seafarer industry as crews are often required at short notice.
- MIPs that hold an MSP sponsoring MSIC applicants was also raised. OTS will include potential sponsoring arrangements in the guidance material.
- Trevor Griffett raised the purpose of the scheme – is the background check or the physical holding of an MSIC the more relevant issue?
- A subcommittee group comprising of Danni Whyte, Dean Summers, Trevor Griffett, Neil Chambers, David Baird, Margaret Fulham, Wynne Jones and members of OTS will meet on 25 February 2005 to discuss the MSIC issues surrounding seafarers, train and truck drivers and casual employees.

Technology:

- John Kilner presented the draft mock MSIC stating that the card would need to include a tamper evident feature and would be a 'smartcard' which would hold biometric information on the card bearer.
- Dean Summers advised that the MUA are opposed to the capturing of biometric information on the MSIC.
- The Working Group discussed that no biometric standard has been established and that the incorporation of biometrics onto the card at this point adds further difficulties to a card that is being resisted by industry.
- Agreement was reached that at this stage the MSIC would no include a biometric.
- The Working Group stated that:
 1. there is currently no biometric standard agreed to worldwide;
 2. employers want to be able to utilise the substrate of the card for access control;
 3. the tamper evident feature must not impact on the substrate of the card;
 4. there is strong resistance from the workforce regarding the capturing of biometrics;
 5. industry do not want an increase in the cost in the card with the inclusion of biometrics; and
 6. industry will undertake to work with the government before the first re-issue phase to investigate the capturing of biometrics.

Lunch and Close of Meeting

LIST OF DISQUALIFYING AND EXCLUSION CR
RELATING TO THE MSIC

Crimes against Humanity:

- Immigration offences

Offences against the country:

- An offence against Part 5 of the Criminal Code
- Serious crimes involving interference with aviation and/or maritime transport infrastructure
- Serious crimes against the Commonwealth or State or Territory or a country other than Australia
- Any violation relating to the sale, delivery, or use of weapons of mass destruction (chemical, biological and radiological)
- Immigration offences

Offences against public order:

- Any offence relating to smuggling, production, supply, import or export of a trafficable amount of explosives, firearms and other weapons, drugs or narcotics, and hazardous material.
- Crimes involving a bomb threat

Theft and similar offences:

- Identity crimes
- Transnationals crime

Unspent convictions:

- Any crimes with a sentence of longer than 30 months
- Any crime which occurs during a ten-year timeframe for re-offenders

Type of Crime	Examples of Crimes	Disqualifying/Exclusion
Any offence against Part 5 of the <i>Criminal Code</i>	Treason, Espionage, Terrorism, Harming Australians	Disqualifying ¹
Any offence relating to the smuggling, production, supply, import or export of a trafficable amount of explosives, firearms and other weapons, drugs or narcotics, and hazardous material	Smuggling of firearms, Smuggling of explosives, Importing or exporting of any drugs or narcotic	Exclusion ²
Any violation relating to the sale, delivery, or use of weapons of mass destruction (chemical, biological and radiological)	Involvement in the sale of a weapon of mass destruction, Use of a weapon of mass destruction against a nation or people of a nation	Disqualifying
Crimes involving a bomb threat	Advancing a political, ideological or religious cause by placing a bomb or bomb threat	Disqualifying
Serious crimes against the Commonwealth or State or Territory or a country other than Australia	Treachery, Sabotage, Sedition, Inciting mutiny, Destroying or damaging Commonwealth property ³ , crimes involving association with Unlawful associations ³ , Unlawful drilling (training) ³	Exclusion
Serious crimes involving interference with aviation and/or maritime transport infrastructure	Hijacking of an aircraft or ship, Destruction of an aircraft or ship, Illegal carriage of Dangerous Goods on board an aircraft or ship, Endangering the security of aerodromes or ports	Exclusion
Identity Crimes	Crimes involving counterfeiting or falsification of identity documents, Assuming another individuals identity	Exclusion
Transnationals crime	Money laundering, Other crimes association with organised crime or racketeering	Exclusion
Immigration violations	People smuggling, Criminal deportation	Exclusion
Any conviction greater than 30 months ⁴	Unspent convictions under Commonwealth Spent Convictions Scheme	Exclusion
Repeat offender who commits a crime within every ten years ⁵	Unspent convictions under Commonwealth Spent Convictions Scheme	Exclusion

Notes:

- ¹ 'Disqualifying' offences are a smaller subset of 'Exclusion' offences. A 'Disqualifying' crime is one which will prevent an employee from holding an MSIC. These crimes are considered serious and would impact directly on the security outcome of the MSIC.
- ² 'Exclusion' offences are those which exclude the sentence from the Commonwealth *Spent Conviction Scheme*. Effectively this means that a criminal conviction in this category will be made available through police records checks even if the offence was committed more than 10 years ago. The impact of a conviction of this nature on the issue of an MSIC would depend on a number of factors including gravity of the particular conviction and whether the applicant is a repeat offender.

Reports on all convictions whether 'Exclusion' or 'Disqualifying' will be provided to DOTARS or the Issuing Body depending on whether the applicant is an existing or new employee.

The Issuing Body or DOTARS depending on whether the applicant is an existing or new employee in the first MSIC round, will have discretionary power to issue an MSIC if the crime is considered to be an 'Exclusion' crime or crimes that have been committed in the last ten years.
- ³ The definitions for these crimes are from Part II of the *Crimes Act 1914*.
- ⁴ Under the Commonwealth Spent Conviction Scheme, any conviction with a prison sentence greater than thirty (30) months is not spent and will be released through a police records check.
- ⁵ Records for repeat offenders – those who are repeatedly sentenced within a ten year timeframe will be beyond the protection of the Spent Convictions Scheme. In that regard, such an offender may have their full criminal history revealed to the Issuing Body back to their first offence depending on the time between each offence/sentence.

Additional note: All personnel including persons of foreign citizenship who are required to have an MSIC will also be required to undergo background checks.

From: Popple Gay on behalf of MarsecID
Sent: Friday, 10 June 2005 5:11 PM
To: 'aimpe@ozemail.com.au'; 'b.beech@patrick.com.au'; George Davis;
'john.allan@twu.com.au'; 'lbgavin@bigpond.net.au'; 'neil@vta.com.au';
'sblackwell@aapma.org.au'; 'danni.whyte@twu.com.au';
'geoff.toomer@amsa.gov.au'; 'Jock.O'Hagan@poports.com.au';
'leanne.lomas@afp.gov.au'; 'lrussell@shippingaustralia.com.au';
'mfulham@adsteam.com.au'; 'mike.william@dpi.wa.gov.au';
'paul.newton@customs.gov.au'; 'pshepherd@sydneyports.com.au';
'Russell.Rowell@afp.gov.au'; 'trevor.griffett@asa.com.au';
'kvanbarneveld@rtbu-nat.asn.au'; 'dsanders@appea.com.au';
'mmccallum@appea.com.au'; 'smorris@cbfca.com.au'; 'SAA@asio.gov.au';
'jbmoller@optusnet.com.au'; Dean Summers
Cc: Liubestic Patricia; Kilner John; Killesteyn Tim; Henderson Carrie -
Anne; Pau Cornelius; Owen Sharyn; Gottlob Roger
Subject: Circulation of draft regulation for Maritime Security
Identification Card

Categories: UNCLASSIFIED
Attachments: 0506243A-050610C.pdf
Titus Classification: UNCLASSIFIED
Classification: UNCLASSIFIED

MSIC Working Group Members,

Please find attached, for your information and comment the draft regulations for the Maritime Security Identification Card. As indicated these are only in draft form as we continue working on them. We would appreciate your comments on these draft regulations by COB 20 June 2005. This will allow us time to take your comments into consideration before the final draft is delivered to you at the next meeting of the working group in the week of 27 June - 1 July.

Should you have any queries please don't hesitate to call me.

Patricia Liubestic

Director, Maritime Security Identity

Office of Transport Security

Department of Transport and Regional Services

GPO Box 594, Canberra, ACT 2601

phone: 02/6274 6254 mobile: 0421 617 491

email: patricia.liubestic@dotars.gov.au

From: Popple Gay
Sent: Monday, 27 June 2005 11:24 AM
To: 'b.beech@patrick.com.au'; George Davis; 'john.allan@twu.com.au';
'lbgavin@bigpond.net.au'; 'neil@vta.com.au'; 'sblackwell@aapma.org.au';
'danni.whyte@twu.com.au'; 'geoff.toomer@amsa.gov.au';
'Jock.O'Hagan@poports.com.au'; 'leanne.lomas@afp.gov.au';
'lrussell@shippingaustralia.com.au'; 'mfulham@adsteam.com.au';
'mike.williams@dpi.wa.gov.au'; 'paul.newton@customs.gov.au';
'pshepherd@sydneyports.com.au'; 'Russell.Rowell@afp.gov.au';
'trevor.griffett@asa.com.au'; 'kvanbarneveld@rtbu-nat.asn.au';
'dsanders@appea.com.au'; 'mmccallum@appea.com.au'; 'smorris@cbfca.com.au';
'SAA@asio.gov.au'; 'jbmoller@optusnet.com.au'; Dean Summers;
'mbyrne@aimpe.asn.au:'
Subject: RE: Papers for MSIC Working Group Meeting - Tuesday 28 June

Categories: UNCLASSIFIED
Attachments: 0506243A-050627A (2) V3.pdf
Titus Classification: UNCLASSIFIED
Classification: UNCLASSIFIED

MSIC Working Group members,

As advised by Patricia please find attached the latest version of the regulations. These regulations are still in draft format and will be settled by the drafter post the working group meeting. They are for discussion on policy issues.

Kind regards

Gay Popple
Maritime Security Identity
Office of Transport Security
Department of Transport and Regional Services
É: 02 6274 6211
Ê: 02 6274 7994
>: gay.popple@dotars.gov.au

From: Henderson Carrie - Anne
Sent: Monday, 27 June 2005 10:57 AM
To: Popple Gay
Subject: FW: Papers for MSIC Working Group Meeting - Tuesday 28 June
Importance: High

Classification: UNCLASSIFIED

From: Liubestic Patricia
Sent: Friday, 24 June 2005 5:37 PM
To: 'b.beech@patrick.com.au'; George Davis; 'john.allan@twu.com.au';
'lbgavin@bigpond.net.au'; 'neil@vta.com.au'; 'sblackwell@aapma.org.au';
'danni.whyte@twu.com.au'; 'geoff.toomer@amsa.gov.au';
'Jock.O'Hagan@poports.com.au'; 'leanne.lomas@afp.gov.au';
'lrussell@shippingaustralia.com.au'; 'mfulham@adsteam.com.au';
'mike.williams@dpi.wa.gov.au'; 'paul.newton@customs.gov.au';
'pshepherd@sydneyports.com.au'; 'Russell.Rowell@afp.gov.au';

'trevor.griffett@asa.com.au'; 'kvanbarneveld@rtbu-nat.asn.au';
'dsanders@appea.com.au'; 'mmccallum@appea.com.au'; 'smorris@cbfca.com.au';
'SAA@asio.gov.au'; 'jbmoller@optusnet.com.au'; Dean Summers;
'walrb@bigpond.net.au'; 'mbyrne@aimpe.asn.au';
Cc: 'todd.frew@immi.gov.au'; Sambrook Jason; Bull Warwick; Henderson Carrie
- Anne; Power Allison
Subject: Papers for MSIC Working Group Meeting - Tuesday 28 June
Importance: High

Classification: UNCLASSIFIED

MSIC Working Group members

In preparation for the MSIC Working Group meeting on Tuesday 28 June please find attached

1. Revised Agenda
2. List of meeting attendees
3. Agenda Item 2
4. Agenda Item 2 - Attachment A - List of major regulations issues raised by working group members

On Monday 27 June, a new draft set of regulations will be emailed out to all working group members. On Tuesday 28 June, we will provide all members with a consolidated list of all comments received and actions undertaken.

Thank you

Patricia Liubestic
Director, Maritime Security Identity
Office of Transport Security
Department of Transport and Regional Services

GPO Box 594, Canberra, ACT 2601
phone: 02/6274 6254 mobile: 0421 617 491
email: patricia.liubestic@dotars.gov.au

From: Popple Gay on behalf of MarsecID
Sent: Friday, 8 July 2005 1:20 PM
To: 'b.beech@patrick.com.au'; 'danni.whyte@twu.com.au';
'david.baird@amsa.gov.au'; Dean Summers; 'geoff.toomer@amsa.gov.au'; George Davis; 'Jock.O'Hagan@poports.com.au'; 'john.allan@twu.com.au';
'Leanne.Lomas@afp.gov.au'; 'lbgavin@bigpond.net.au';
'lrussell@shippingaustralia.com.au'; 'mfulham@adsteam.com.au';
'mbyrne@aimpe.asn.au'; 'neil@vta.com.au'; 'paul.newton@customs.gov.au';
'pshepherd@sydneyports.com.au'; 'smorris@cbfca.com.au';
'sblackwell@aapma.org.au'; 'SAA@asio.gov.au'; 'trevor.griffett@asa.com.au';
'Wynne.Jones@woodside.com.au'; 'k.hamilton@patrick.com.au';
'kvanbarneveld@rtbu-nat.asn.au'; 'jbmoller@optusnet.com.au';
'mmccallum@appea.com.au'; 'dsanders@appea.com.au';
'mike.williams@dpi.wa.gov.au'; 'jennifer.robinson@customs.gov.au';
'graham.leary@afp.gov.au'; 'jhirst@aapma.org.au'; 'john@amou.com.au'
Cc: Henderson Carrie - Anne; Liubestic Patricia
Subject: FW: MSIC Regulations

Importance: High

Categories: UNCLASSIFIED

Attachments: Draft Minutes - 28 June 05.doc; 0506243A-050707B.pdf

Titus Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

MSIC Working Group

Attached for your information is a copy of the final MSIC regulations. In order for these regulations to be made at the meeting of the Executive Council on 21 July, we will not be able to accept any more amendments to this version.

I have also attached for your information a copy of the draft minutes from the MSIC Working Group Meeting of 28 June 2005 and would appreciate any comments you might have by COB Friday 22 July 2005.

Thank you all for your contributions to developing the MSIC regulatory framework.

Patricia Liubescic
Section Head, Maritime Security Identity
Office of Transport Security
Department of Transport and Regional Services

GPO Box 594, Canberra, ACT 2601
phone: 02/6274 6254 mobile: 0421 617 491
email: patricia.liubescic@dotars.gov.au

Answer to Question 6

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

“How many of those [staff who are transport security inspectors] in the state offices, would regularly visit these workplaces as well as do their other duties?”

The answer to the honourable member's question is as follows:

- All state based staff are transport security inspectors.
- The number in each state varies and the number of staff in the state offices is growing, but to give an indication of numbers of staff who regularly do Audit and Compliance functions in the Maritime Sector are as follows :
 - **QLD** Has 5 inspectors including a Master Mariner with over 30 years experience in commercial maritime operations
 - **NSW** Has 4 maritime security inspectors
 - **VIC/TAS** Has 9 inspectors, several inspections are done per week by the office, mostly conducted on ships
 - **SA/NT** Has 3 Maritime based inspectors in SA, and 1 in NT
 - **WA** Has 4 Maritime based inspectors. Due to the nature of work in WA, when undertaking audits of ports and airports outside of Perth, both Maritime and Aviation based inspectors will undertake audits in the port, then the airport in the same trip.

Answer to Question 7

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

“Draft regulation 6.07M provides for the secretary of the Department of Transport and Regional Services to exempt certain persons or classes of persons from holding, carrying or displaying an MSIC. This is not a reg that concerns the defence forces or emergency services personnel that are dealt with in 607J2(b) and 6.07N. What persons or classes of persons will be eligible to receive this exemption?”

The answer to the honourable member's question is as follows:

- Regulation 6.07M provides that persons may be exempted by the Secretary from the requirement to hold, carry or display an MSIC. Applications can be made for an individual, or a class of persons. Some examples of why this exemption can be applied for include:
 - OH&S- If it is dangerous for a person to wear an MSIC, an individual, maritime industry participant or offshore industry participant can apply for an exemption to display an MSIC, however they will still need to carry it within a maritime security zone. In this instance an application can also be made for exemption to display or carry an MSIC, but they will still need to hold an MSIC.
 - In case of an emergency, such as an oil spill, an application can be made for persons entering the zone (or part of the zone) who are enabling clean up efforts to apply for exemption to hold, carry or display an MSIC, thus removing the requirement for an MSIC or an escort for people in those situations.
- When applying for an exemption, and when the secretary is approving or declining an application for exemption the following must be considered:
 - why the exemption is necessary,
 - the likely effect of any exemption,
 - the length of time of any exemption
- The Secretary can give an exemption for a particular period and with any conditions including limitations to particular zones or areas of zones.
- During the hearing, witnesses expressed concern to the committee that there are not adequate arrangements for people to access a maritime security zone in the case of an environmental emergency such as an oil spill. In emergencies such as these, maritime industry participants or offshore industry participants can apply and receive an exemption from people wearing MSICs in a certain maritime security zone, or an area of a maritime security zone. An exemption can be applied for by contacting the Office of Transport Security's 24 hour operations centre, which can facilitate urgent requests for exemptions from the MSIC scheme in cases of emergency.

Answer to Question 8

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005:

Why should those persons who have been issued a disqualifying notice under 6.07K(1) be allowed to enter a zone unescorted for the purpose of boarding or leaving vessel as part of a recreational activity unescorted?

The answer to the honourable member's question is as follows:

UNDER REGULATION 6.07K A PERSON WHO HAS BEEN ISSUED A DISQUALIFYING NOTICE MAY ENTER A MARITIME SECURITY ZONE AS A VISITOR FOR THE PURPOSE FOR BOARDING OR LEAVING A VESSEL AS PART OF A RECREATIONAL ACTIVITY.

REGULATION 6.07I PROVIDES A DEFINITION FOR VISITOR AND ESCORT AND REGULATION 6.07J(2) PROVIDES THAT A VISITOR MUST BE ESCORTED OR CONTINUOUSLY MONITORED BY AN MSIC HOLDER. THEREFORE ANY PERSON WHO IS A VISITOR TO A MARITIME SECURITY ZONE MUST BE EITHER ESCORTED OR CONTINUOUSLY MONITORED.

Answer to Question 9

Senator O'Brien asked the Office of Transport Security, on: Tuesday 12 July 2005.

"Can the committee be provided with a breakdown of costs associated with the introduction of the MSIC, and the extension of the maritime security regime to offshore facilities?" **The answer to the honourable member's question is as follows:**

The question needs to be broken down into three separate responses

1. The cost to industry for the introduction of the MSIC.

- In the implementation phase MSIC Issuing Bodies will be responsible for;
 - establishing an MSICs identity based on the 100 point methodology
 - verifying there is a legitimate need for the MSIC
 - providing a conduit for the consent to conduct background checks between the applicant and AFP and ASIO; and
 - manufacturing and issuing an MSIC
- Based on the Aviation Security Identification Card (ASIC) Scheme it is anticipated that there would be the following basic establishment costs.

○ Card Printing Machine	○ \$10,000
○ Tamper Evident Feature (TEF) Printing Machine	○ \$19,000
○ Storage Systems	○ \$ 5,000
○ Digital Camera	○ \$ 1,500
○ Total	○ \$35,500

- There would be additional cost associated with consumables required for the cards
 - Cards
 - Ink
 - Clips/lanyards
 - Materials for the TEF (approximately 25cents per card)
 - Stationary.
- There would be costs associated with additional staff & accommodation required to process the applications.
- It is anticipated the cost of MSIC production may be reduced if an issuing body has an existing access card system in place where the substrate card can be used to add the MSIC feature to it (advice in each case would need to be sought from the TEF provider). If this is the case the requirement for an additional card printing machine would no longer be necessary.

2. The cost to the individual for the introduction of the MSIC.

- Based on the aviation model, some employers will absorb the costs of the MSIC for their employees while other will pass the costs onto their employees.
- The cost of the ASIO and AFP checks are \$49 at this stage, however the fee charged by the AFP is being reviewed. We anticipate that there maybe an increase over time.
 - AFP Criminal History Check - \$36
 - ASIO PMV check - \$13
- It is anticipated the cost of an MSIC will be approximately \$150 based on the Aviation Security Identification Card (ASIC), however the final cost will be determined by the MSIC Issuing Body.
- An applicant will need to prove to the Issuing Body that they are an Australian Citizen or have a valid visa with 'work right' status. They will do this by producing and Australian birth certificate or citizenship/visa documentation. If they don't hold either of these documents there will be a cost associated in obtaining this documentation.
- In addition to the financial cost for an individual they will also a need to
 - Complete and provide the documentation required to obtain an MSIC.
 - During the implementation phase the individual will be responsible for submitting their Police Record Check Consent Form directly to the AFP.
 - If an MSIC is unable to be issued to applicant that person will not be able to work unmonitored in a Maritime Security Zone. The rate of ASIC applicants who were refused an ASIC in the recent reissue was approximately 0.0002%. It is expected the numbers of people refused an MSIC will be similar.
- In the event of an applicant not being able to obtain an MSIC, appeal mechanisms will be incorporated into the regulatory framework. DOTARS envisages a process linked to the Administrative Appeals Tribunal as currently applies under the ASIC Scheme.

3. Extension of the maritime security regime to offshore facilities

- There are two components with respect to this question: the first component is the cost of preparing for the plan and then writing the plan and the second component is the cost of implementing any changes to the current working arrangements in accordance with the plan.
- In both cases there has not been a consistent cross-industry estimation of the costs of either the first or second component. However some industry operators have indicated that they will use consultants to write their security plans and have estimated that that may result in consultancy fees of about \$30,000.
- There have been no figures attributed to the costs of any enhanced security measures by industry. While you can expect there may be some costs, it is likely that any additional costs of security measures at the base security level would be minimal. This is because offshore oil & gas facilities are already very controlled environments – persons are not able to freely gain access as you can freely enter a terminal at an

airport or drive near a port on a public road. So, from a security point of view there are already good access control measures in place for these facilities and those measures have been put in place by the companies to reflect the level of danger associated with petroleum production. As the base operating security level already has access control the costs of any enhanced measures may not be very high.

- These same operators make the point that they can not reliably estimate the costs of an enhanced security regime: it will depend on the preventive strategies that are put in place. These decisions have not yet been made by all of industry. However, they note that where possible some measures will be incorporated in existing work procedures. This is a sensible business decision that would minimise costs and may be open to industry. Also as part of the anecdotal discussion the Offshore Report does note that some members of industry saw that some business costs would be reduced by a formal enhancement of security. In particular they noted that the business process surrounding interaction with security-regulated ships would be stream-lined if their facility was also security-regulated.
- Thus, there has not been a quantitative analysis of costs versus benefits of enhanced security measures. But there is no reason to conclude that the costs will outweigh the benefits for the following reasons:
 - industry has not settled on their preventative strategies (therefore costs can only be an estimate);
 - they will take the sensible business strategy of writing in security considerations to existing business procedures, presumably, where possible (they will minimise cost).

Answer to Question 10

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

"The committee heard evidence that a small number of industry participants have abused the maritime security regime to achieve other objectives, including preventing representatives of the International Transport Workers Federation from communicating with ships crews. In May Mr Kilner told the committee that the department had investigated two complaints related to this issue. What was the outcome of those investigations?"

The answer to the honourable member's question is as follows:

- DOTARS has investigated two complaints about industry participants abusing the maritime security regime to prevent access by representatives of the International Transport Workers Federation.
- One of these complaints related to access to a port facility. The International Ship and Port Facility Security Code and the Maritime Transport and Offshore Facility Security Regulations require that Port Facility Security Plans address procedures for facilitating access by visitors, including representatives of labour organisations. This is to ensure that security plans are not used to prevent otherwise legitimate access. All security plans approved under the Regulations, including the security plan for the port facility in question, meet this requirement.
- The second complaint related to access to a ship. OTS understand that the master of the ship in question claimed his ship was operating at security level 2, and that operating at security level 2 was grounds for denying access to the ship by ITF representatives.
- Under the SOLAS Convention, the master of a ship may implement such measures to protect the safety and security of the ship as are deemed necessary. This may include denying access to persons whose access is not otherwise mandated, on the grounds of "security". However denying access on the grounds of operating at security level 2 would only be reasonable if the ship is in fact at security level 2.
- Only a Contracting Government to the SOLAS Convention can raise a ship's security level, and there is no evidence that the ship's Flag Administration had raised the ship's security level on this occasion. We have sought an explanation from the ship's Flag Administration as to the level at which the ship in question was operating at the time.
- DOTARS considers the making of a false declaration about the security level at which a ship is operating to be an inappropriate use of the maritime security regime. If it becomes clear, following the conclusion of the current investigation, that the master of the ship in question has acted inappropriately, DOTARS will pursue the matter both with the Flag Administration, and with the International Maritime Organization.

Answer to Question 11

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

“Can you advise the committee whether or not any deficiency in the administration of the coastal shipping permit system has been identified by any internal or external audit?”

The answer to the honourable member's question is as follows:

- An internal audit report was undertaken by KPMG as an initiative of the Department of Transport and Regional Services between June and August 2004.
- The Department commissioned this review at a time when processing responsibility was being handed over to the Office of Transport Security. The auditors were asked to assess whether the existing departmental arrangements ensured compliance with relevant requirements and in what ways the processing system could be improved.
- Overall, the audit report noted that the existing arrangements generally ensured compliance, but that records management practices in place at the time the audit was conducted reduced the ability of the Department to demonstrate this compliance.
- The recommendations have been addressed through changes in procedures for processing permits and licences, changes in records management practices and as part of a broader rewrite of the Coasting Trade Regulations. These amendments are close to finalisation.

Answer to Question 12

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

"Do we know how many of those crew [the 200,000 foreign seafarers that enter Australian ports each year] are from flag of convenience vessels?"

The answer to the honourable member's question is as follows:

- The term "flag of convenience" does not refer to an officially recognised category of vessels, and we are unable to provide information regarding such vessels, or their crews.

Answer to Question 13

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 :

“One of the issues raised in the joint union submission to this inquiry, and identified as a security gap in the ASPI report, is poor container security. We are told that no empty containers are screened, but how many empty containers are brought through Australian ports each year?”

The responsibility for screening of containers (primarily in bound) lies with the Australian Customs Service. DOTARS has consulted with the Australian Customs Service regarding the Honourable Members question, and is waiting for an answer.

Answer to Question 14

Senator Sterle asked the Office of Transport Security on Tuesday 12 July 2005:

“Will DOTARS give an undertaking to let members of the working group have a further opportunity to comment quickly on the latest draft regulations?”

The answer to the honourable member's question is as follows:

- The Department of Transport and Regional Services recirculated the draft MSIC regulations on 26 July 2005 to the Working Group. At this time an invitation to either meet or hold a teleconference on 4 or 9 August 2005 to discuss the draft MSIC regulations was offered to the Working Group. Most Working Group members have responded indicating a preference for attendance at the proposed 9 August meeting.

Answer to Question 15

Senator O'Brien asked the Office of Transport Security on Tuesday 12 July 2005 to clarify what regime is in place to check for the transport of things like ammonium Nitrate by foreign flagged ships.

The answer to the honourable member's question is as follows:

- When an application for an Single Voyage Permit (SVP) or a Continuous Voyage Permit (CVP) is lodged and as part of the application assessment process, the Office of Transport Security (Operations Centre) ensures that the vessel meets with all requirements of the Maritime Transport Security Act and the International Ship and Port Security Code. The application for an SVP or CVP lists the type of cargo to be carried and the estimated amount to be moved. Once the application is approved and the Permit issued, this is passed onto the Australian Customs Service.

The Honourable Member also wanted to know how to confirm the information provided in the SVP or CVP is correct. DOTARS is waiting on an answer from the Australian Customs Service for an answer to the Honourable Members question.



Australian Government

Department of Transport and Regional Services

OFFICE OF TRANSPORT SECURITY
GPO Box 594 Canberra ACT 2601 Australia

• Telephone: 02 6274 7111 • Facsimile: 02 6274 7994 • Operations Centre 1300 307 288
Website: www.dotars.gov.au • ABN 86 267 354 017

Answer to Question 16

Senator Webber asked the Office of Transport Security on Tuesday 12 July 2005 :

“Regarding the people who access the maritime security zones and do not have an MSIC, they get escorted around or they can be monitored by closed circuit television? Do the people monitoring them on the closed circuit television on a continuous basis have to hold an MSIC?”

The answer to the honourable member's question is as follows:

- An escort, which by the definition in 6.07I is a person which escorts, or continuously monitors another person in a maritime security zone.
- Regulation 6.07J (2) states that the requirement to display an MSIC in a maritime security zone does not apply to a visitor to the zone, if his or her escort is:
 - displaying a valid MSIC,
 - carrying a valid MSIC, but is exempt from the requirement to display it,
 - exempt from carrying the MSIC (but still holds one).
- Therefore, the requirement in the regulations is for a visitor to be continuously monitored or escorted by an MSIC holder, regardless of whether that ‘escort’ is inside or outside of the maritime security zone, and whether they are physically escorting them or monitoring them via closed circuit television.