The Senate

Rural and Regional Affairs and Transport Legislation Committee

Regulatory framework under the *Maritime Transport Security Amendment Act 2005*

August 2005

ISBN 0 642 71565 3

This document was prepared by the Senate Rural and Regional Affairs and Transport Legislation Committee, and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Membership of the Committee

Members

Senator the Hon. Bill Heffernan	LP, New South Wales	Chair
Senator Jeannie Ferris	LP, South Australia	
Senator Anne McEwen	ALP, South Australia	
Senator Julian McGauran	NPA, Victoria	
Senator Christine Milne	AG, Tasmania	
Senator Glenn Sterle	ALP, Western Australia	

Participating Members

Senator Abetz	Senator Eggleston	Senator Mason
Senator Allison	Senator Evans	Senator McLucas
Senator Bartlett	Senator Faulkner	Senator Nettle
Senator Bishop	Senator Ferguson	Senator O'Brien
Senator Boswell	Senator Hogg	Senator Payne
Senator Brown	Senator Hutchins	Senator Ray
Senator G Campbell	Senator Lightfoot	Senator Santoro
Senator Carr	Senator Ludwig	Senator Stephens
Senator Chapman	Senator Lundy	Senator Watson
Senator Coonan	Senator S MacDonald	Senator Webber
Senator Crossin	Senator Mackay	

Committee Secretariat

Ms Maureen Weeks, Secretary
Ms Sharon Babyack, Research Officer
Ms Rosalind McMahon, Executive Assistant

Parliament House, Canberra
Telephone: (02) 6277 3511
Facsimile (02) 6277 5811

Internet: www.aph.gov.au/senate
Email: rrat.sen@aph.gov.au

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AAPMA	Association of Australian Ports and Marine Authorities Incorporated
AFP	Australian Federal Police
AIMPE	Australian Institute of Marine and Power Engineers
AMWU	Australian Manufacturing Workers Union
ASA	Australian Shipowners Association
ASIC	Aviation Security Identity Card
ASIO	Australian Security Intelligence Organisation
CCTV	Closed Circuit Television
DIMIA	Department of Immigration, Multicultural and Indigenous Affairs
DOTARS	Department of Transport and Regional Services
EM	Explanatory Memorandum
MIP	Maritime Industry Participant
MSIC	Maritime Security Identity Card
MSZ	Maritime Security Zone
MTSA 2003	Maritime Transport Security Act 2003
MTSA Act	Maritime Transport Security Amendment Act 2005
MUA	Maritime Union of Australia
NPP	National Privacy Principles
RTBU	Rail, Tram and Bus Union
OH&S	Occupational Health and Safety
OTS	Office of Transport Security
TWU	Transport Workers Union

Chapter 1

The Committee's Inquiry

Conduct of the Inquiry

1.1 On 16 June the Senate referred to the Rural and Regional Affairs and Transport Legislation Committee the regulatory framework to be implemented and enforced by DOTARS under the *Maritime Transport Security Amendment Act 2005* for inquiry and report.[1] Specifically, having regard to:

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

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.

1.2 The committee advertised the inquiry in *The Australian* on 22 June and 6 July 2005, and wrote to a number of organisations inviting submissions. The committee received 13 submissions (see Appendix 1) and held a public hearing on Tuesday 12 July 2005 (see Appendix 2).

1.3 The committee acknowledges and thanks submitters and witnesses for their contribution. Submissions and the *Hansard* transcript of the committee hearing is available on the Parliament's webpage at http://www.aph.gov.au.

Purpose of the Amending Act

1.4 The first part of the *Maritime Transport Security Amendment Act 2005* (MTSA Act) extends the *Maritime Transport Security Act 2003* (the principal Act) to apply to Australia's offshore oil and gas facilities. These facilities are located within the defined areas of Australia's territorial sea, exclusive economic zone and continental shelf. The main purpose of the Act is to regulate the offshore oil and gas industry's security arrangements. This includes the requirement of industry

---

1 *Journals of the Senate*, 16 June 2005, p. 708

participants to develop and comply with security plans specifically tailored to each facility based on security assessments.[2]

1.5 The second part of the MTSA Act amends the principal Act to allow for the introduction of the Maritime Security Identification Card (MSIC). It is this part of the MTSA Act that was the focus of the committee's inquiry. Personnel working unmonitored in the Maritime Security Zones (MSZ)[3] and offshore security zones[4] will be required to hold and display MSICs. Applicants for the MSIC will undergo a background, including criminal, check. An applicant's criminal check must meet certain requirements to enable them to receive the MSIC. The scheme is provided for in the MTSA Act, and is established by regulations.

The Maritime Security Identification Card (MSIC)

1.6 The Explanatory Memorandum (EM) to the MTSA Act outlines that there is currently no requirement to 'confirm the character and identity of those entering a [MSZ]'.[5] This limits the knowledge of who accesses sensitive port and ship areas. It also increases the risk of terrorist activities on maritime infrastructure via legitimate access to the MSZs. The government contends that imposing the MSIC regime will have a 'significant deterrent effect' on terrorist organisations that might seek to attack maritime targets of convenience.

1.7 The MSIC will serve as an identity card only and will not provide access to secure areas within the zones. It will however allow personnel working in MSZs and offshore security zones to be identified at any given time. A representative of the Association of Ports and Marine Authorities Inc. (AAPMA) clarified this in evidence given during the committee hearing:

> There will be a separate access card, and that certainly is getting more sophisticated as we go on... [The MSIC] is a photographic ID. It is not an access card. You can build access into the back of the card. There is a substrate that will take access… The identity card will not be a swipe card like an access card, unless it has access provisions built into it. [The MSIC] is an ID card only. It just says that the person has had a certain level of security checks run on them and that they are who the card says they are.[6]

1.8 The Department of Transport and Regional Services (DOTARS) confirmed this in its submission:

---

2 Explanatory Memorandum, p. 2

3 The MSZ is comprised of ports, ships, and on board security zones as declared under subsections 102(1), 106(1) and 110(1) of the MTSA Act respectively.

4 Offshore facilities are defined in the MTSA Act under s113A(1) as areas declared by the Secretary, within and around an offshore facility.

5 Explanatory Memorandum, p. 24

6 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 30

> 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.[7]

The Regulations

1.9 Two sets of regulations are proposed under the amending Act. The Maritime Transport Security Amendment Regulations 2005*,* which relates to the extension of the MTSA 2003 to offshore oil and gas facilities; and the Maritime Transport Offshore Security Amendment Regulations 2005 draft which relates to the administration of the Maritime Security Identification Card (MSIC).

1.10 The committee's inquiry examined how the regulations pertaining to the MSIC protect privacy interests and the cost recovery measures for the card. The committee also investigated how the card will be issued and displayed and how the regulations related to the MSIC will be enforced. In addition, the security checks for foreign seafarers were examined.

1.11 The inquiry is based around Division 6.1A of the regulations which provide for the issue of the MSIC to identify a person who has been the subject of a background check. A maritime industry participant (MIP) will not allow a person access to a maritime security zone unless he or she displays a valid MSIC or is escorted by a MSIC holder. Division 6.1A includes requirements about the display, issue, expiration and cancellation of the MSIC. Further, it addresses the criteria of Issuing Bodies (IBs) of the MSICs.[8]

1.12 Some of the provisions of the regulations addressed during the committee's inquiry are as follows;

- Table 6.07C, *Maritime-security-relevant offences* in Division 6.1A outlines disqualifying and exclusion offences that are used to assess the criminal background of a MSIC applicant.[9]
- Regulation 6.08C(2) states that from 1 October 2005 to 30 June 2006 the Secretary of the Department of Transport and Regional Services (DOTARS) will decide whether the criminal record check shows that a MSIC applicant

---

7 Submission No. 13, *Department of Transport and Regional Services,* p. 3

8 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 4

9 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 6

has an adverse criminal record. Following this period, Issuing Bodies (IBs) will make the decision.[10]

- Subdivision 6.1A.2, *Display of MSICS,* outlines the penalties applied if a MSIC holder does not properly display their card in a maritime security zone. It also outlines the requirements to escort a visitor to a maritime security zone, and the penalties issued if the requirements as an escort are not fulfilled.[11]
- Regulation 6.07M allows for a person to be exempted from the requirement to hold, carry or display an MSIC.[12]
- Regulation 607J2(b) and 6.07N which allow for members of the Defence Force and ambulance, rescue or fire service officers to enter a maritime security zone without displaying an MSIC.[13]
- Regulation 6.07G provides for maritime industry participants, a body representing participants, a body representing employees of participants and Commonwealth authorities to be authorised as Issuing Bodies.[14]
- Subdivision 6.1A.6, *Record Keeping,* outlines how an IB must keep a register of MSICs and how IBs must retain the record of issue of all MSICs for 7 years. [15]
- Subdivision 6.1A.8, Regulation 6.09A, *Cost Recovery,* states that an IB may recover the reasonable costs of the issue of the MSIC from the applicant for an MSIC.[16]

1.13 The above regulations are examined in greater detail in Chapter 2, *Implementation* and Chapter 3, *Administration*.

---

10 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 23

11 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, pp. 11-4

12 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 13

13 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, pp. 11 and 14

14 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 14

15 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, pp.34-5

16 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 38

Chapter 2

Implementation

Introduction

2.1 The provisions of the *Maritime Transport Security Amendment Act 2005* (MTSA Act) and the associated regulatory framework represents a further plank in the roll out of security measures designed to protect Australia's transport system and critical infrastructure from terrorist threat. The MTSA Act extends the *Maritime Transport Security Act 2003* (the principal Act) to Australia's offshore oil and gas facilities. It is a formalised approach to enhance security arrangements on fixed and floating offshore facilities and port facilities.

2.2 During the inquiry, there was general support for the aim of the legislation and the measures it establishes, including the MSIC. The unions noted that it is their membership who are likely to be the human victims of any terrorist attacks on wharves or off shore facilities.[1] However, within the committee's terms of reference there were of number of concerns raised by those involved in the development and implementation process. These concerns addressed the level of consultation undertaken with industry participants in relation to the MSIC; privacy issues and also means of cost recovery for the card.

Consultation

2.3 During the inquiry, considerable comment was made relating to the adequacy of the consultation process.

2.4 The committee learnt that the consultation process commenced in September 2004 with the Department of Transport and Regional Services (DOTARS) holding a seminar to discuss the MSIC with maritime industry participants. This seminar was followed in the next month with the formation of a smaller working group, with DOTARS as chair. This working group met regularly after its formation.[2]

2.5 Other dates of significance in the consultation process include:

- February 2005, 'List of disqualifying and exclusion crimes relating to the MSIC' given to the working group.[3]

- April 2005, maritime industry meeting where further industry participants were invited to become part of the working group.

---

1 Submission No. 8, MUA, RTBU, AMWU, p. 4

2 Submission No. 10, AAPMA, p. 2

3 DOTARS, *Hansard,* 12 July 2005, p. 57

- 10-12 May 2005, DOTARS officers visited offshore oil and gas operators and the Australian Petroleum Production and Exploration Association (AAPEA) to consult on the MSIC regime.

- Early June 2005, the first set of draft regulations were issued to the working group.

- Late June 2005, face-to-face meetings with working group members. Members of the working group were advised that the next set of draft regulations to be circulated would be presented to the Executive Council on 21 July 2005.

- 27 June, a set of revised regulations were made available to the working group participants.[4]

- 8 July 2005, the third draft regulations were released and consultation was officially drawn to a close via email notification.

2.6 Witnesses who appeared before the committee generally commented on the consultation process and commended the department on their efforts in the early part of the process. The Association of Australian Ports and Marine Authorities (AAPMA) indicated that:

> The working group have accomplished a significant amount of work and we are a very flexible group; we respond to the unfortunate events that occur from time to time. … As we have all noted this morning, it has provided a tremendous level of trust and communication amongst all the parties in the maritime environment.[5]

2.7 However, not all participants were satisfied with the process. The Rail, Tram and Bus Union (RTBU) believe it had been involved too late in the process[6] and the Australian Manufacturing Workers Union (AMWU) commented:

> DOTARS has been incapable of appreciating the value of Union consultation as there were none involved in other important parts of the government's initiatives. Specifically, when the draft legislative amendments to the MTSA to include the offshore industry were presented, Unions and industry alike were taken aback by the lack of any consultation.[7]

2.8 Of greater concern was the lack of consultation with industry and unions for the release of the third draft regulations (8 July regulations). The third draft regulations were distributed at close of business on 8 July 2005, which was one

---

4 Submission No. 13, DOTARS, 'Answers to questions 4 and 5', p. 14 and p. 6

5 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 30

6 Submission No. 8, MUA, RTBU and AMWU, p. 7

7 Submission No. 5, Australian Manufacturing Workers Union, p. 1

working day prior to the committee's hearing. The committee was informed that this action impeded the ability of witnesses to effectively prepare for the hearing.[8]

2.9 During the hearing, the committee also was informed that the e-mail providing the regulations stated:

> 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 able to accept any more amendments to this version.[9]

2.10 This e-mail gave rise to concerns about the efficacy of the committee's inquiry. Given the committee is due to report to the Senate on 9 August 2005, the Maritime Union of Australia, the Rail, Tram and Bus Union and the Australian Manufacturing Workers Union's joint submission voiced concern that the department had no intention of taking the committee's inquiry into consideration when finalising the regulations:

> We are however very concerned that the Government has indicated an intention to finalise the regulations and present them to the Executive Council on July 21 – well before the reporting date of this inquiry. It is the view of these three unions that this undermines the role of the committee, and limits our ability to engage in the policy process of the Australian Parliament.[10]

2.11 Further voice was given to these concerns at the hearing by the TWU representative:

> The instruction that no change will be made post 21 or 22 July sends a pretty clear message about what that department and its officers think of the deliberations of this committee. It pre-empts all the submissions, all the evidence and your own deliberations, so I think scant regard will be paid to this process, if Friday's email is any indication.[11]

2.12 The department responded that this was not their intention:

> CHAIR—I take it that we should not see this [the email] as flying in the face of this process here today?
>
> Mr Tongue—Absolutely not. All we were trying to do was round up a quite extensive process of consultation that we are trying to get done and get comments in from industry so that we can meet some pretty tough deadlines.[12]

---

8 Ms Whyte (TWU), *Hansard,* 12 July 2005, p. 7

9 Email to the MSIC working group from the Section Head, Maritime Security Identity, OTS, DOTARS (undated)

10 Submission No. 8, MUA, RTBU, and AMWU, p. 3

11 Ms Whyte (TWU), *Hansard,* 12 July 2005, p. 13

12 *Hansard,* 12 July 2005, p. 53

2.13 The committee is not reassured by these comments. While it is well aware that regulations can be amended if required at a later date, it does not believe that the department's e-mail can be seen as anything other than a total disregard of the committee's, and indeed the Parliament's process. It has also been an unnecessarily abrupt conclusion to what the committee assesses to have been a productive consultation process and has created confusion amongst participants that may have ramifications for the implementation of the MSIC.

2.14 One impact is the confusion arising out of changes made between the second and third draft of the draft regulations to the meaning of 'maritime security relevant offence.' Draft regulation 6.07 includes a table indicating the kind of offence that would be considered in issuing a MSIC (see appendix 3 for the draft regulations considered by the committee).

Maritime Security Relevant Offences: deciding the level of criminality

2.15 The committee heard from various witnesses that table 6.07C in the 8 July draft regulations did not concur with the working group's agreement on the level of criminality that would constitute the disqualification of an MSIC application.

2.16 In February of 2005 the working group was provided with a copy of a table entitled 'List of disqualifying and exclusion crimes relating to the MSIC'. This document indicates the level of criminality that would constitute disqualification from obtaining a MSIC. In the earlier drafts of the regulations, item 3 of the table referred to section 15HB of the *Crimes Act 1914* (Crimes Act). The 8 July regulations refer instead to offences 'mentioned in Part II of the *Crimes Act 1914'*.[13]

2.17 A representative of the Transport Workers Union (TWU) expressed concern that Part IIA of the Crimes Act could fall within the meaning of Part II contained in table 6.07C. Section 30J of Part II of the Crimes Act includes crimes specifically related to industrial disturbances, lock outs and strikes.[14]

2.18 The TWU argued that the draft regulations:

> potentially completely changes one of the most fundamental issues that the working group has considered—that is, the background checking. There are 30 more crimes against which people's backgrounds will be checked. One of those is interfering with political activity. That alone throws up all sorts of concerns for my organisation. There is an argument to be made, I think, over whether or not part 2A is included in part 2—I do not think that is clear at all. And of course, if we get to that stage, that then picks up

13 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, p. 6

14 *Crimes Act 1914 (Cth),* Part IIA, sec. 30J, pp. 364-5

> industrial disturbances, lockouts and strikes, something that, I can assure you, has never been the subject of deliberations in the working group.[15]

2.19 The hearing provided the opportunity to clarify that Part IIA of the Crimes Act was not intended to be included in the table of maritime security relevant offences:

> Senator O'BRIEN—You have already said this, but I just want to be clear, and I think your view equates with mine—that is, reference to part II of the Crimes Act does not automatically include part IIA of the Crimes Act.
>
> Ms Liubesic—That is exactly right.
>
> Senator O'BRIEN—And you have taken advice on that?
>
> Ms Liubesic—Yes. In fact, it has never been a point of discussion with any member of the working group whether that part was in or out. It was always part II, not part IIA.
>
> Senator O'BRIEN—So you have been talking about part II of the Crimes Act rather than all of it, but certainly none of part IIA?
>
> Ms Liubesic—That is exactly right.[16]

2.20 However, the issues arising from the change from section 15HB of the Crimes Act to Part II remain.

2.21 The AAPMA echoed the unions' concerns that table 6.07C did not reflect the department's working group discussions with industry and the unions:

> I note the committee's interest in the table attached under regulation 6.07C and I also note our interest in item 3 of that—offences mentioned in part II of the Crimes Act 1914. This is completely different from earlier drafts of the regulations and there was no consultation with the working group on that, which I think is regrettable.[17]

2.22 During the hearing, the department's response to the concerns about item 3 fluctuated from indications that it was a drafting error[18] to an admission that it was a change. While indicating that discussions of the working group had been taken into consideration when forming the draft regulations, officers confirmed that it was a Government decision to amend parts of the regulations so that working group consensus was not reflected, particularly in relation to the maritime security relevant offences:

> It is a change. It reflects some decisions that were taken by the government in the context of background checking in the aviation and maritime sector. Whilst we could have talked about it for longer with the industry, my

---

15 Ms Whyte, *Hansard,* 12 July 2005, p. 7

16 *Hansard,* 12 July 2005, p. 59

17 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 27

18 *Hansard*, 12 July 2005, p. 59

> judgment is that it was not going to affect the government's consideration of where it wanted to go with that change.[19]

2.23 In answers to questions taken on notice at the hearing, the department commented that the drafting correction (to omit the reference to section 15HB of the Crimes Act and replace it with Part II) were made in the second draft of the regulations provided to the working group on 27 June 2005. The department continued by indicating that it did not know why 'some members of the working group failed to note the inclusion'.[20]

2.24 The committee notes the department's confusion over the inclusion of Part II in the draft regulations and the fact that clarification only came with time to review its response. It again considers it indicative of the haste in which the final stages of the consultation were undertaken. The committee considers this to be regrettable and to cast doubt over the adequacy of the consultation process.

Operation of Security Checks

2.25 During the committee's hearing consideration of table 6.07C in the draft regulations revealed further matters of concern to the committee. These matters arise from the categorisation of disqualifying offences and exclusionary offences.

Disqualifying or Exclusion?

2.26 Table 6.07C in the draft regulations includes eight items relating to maritime security relevant offences. Of these, items one and two are considered to be offences that would constitute a disqualifying offence for a MSIC applicant. Applicants having either of these offences on their background check would be automatically ineligible for an MSIC. The items are as follows:

> 1. An offence mentioned in Chapter 5 of the *Criminal Code.*
>
> *Note* Offences for this item include treason, espionage and harming Australians
>
> 2. An offence involving the supply of weapons of mass destruction as mentioned in the *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995.* [21]

2.27 The other 6 items are considered exclusionary offences. These will trigger 'amber lights' in assessment of an applicant. These 'exclusion' offences would require further assessment, not automatic disqualification from receiving an MSIC. DOTARS stated:

---

19 Mr Tongue, *Hansard,* 12 July 2005, p. 54

20 Submission No. 13, DOTARS, 'Answers to questions 4 and 5', p. 14

21 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, p. 6

> Exclusion gives us the ability to have a look at the circumstances surrounding the crime. For example, in identity crimes we might pick up somebody who has been caught producing drivers licences and things like that or we might pick up somebody who has committed a more serious identity theft, and we would have the ability to look into the circumstances of that particular crime.[22]

2.28 The committee notes the flexibility to examine the severity of the crime sought under the exclusionary categories. However, exclusionary offences include the crimes that involve 'interference with aviation or maritime transport infrastructure including hijacking of an aircraft or a ship'.[23]

2.29 During the hearing the committee examined the proposal.

> **CHAIR**—So if I were convicted of treachery, sabotage or hijacking an aircraft there would still be a chance that there would be a reason why I hijacked the aircraft that allowed me to go back and work on the wharves—is that the case?
>
> **Ms Liubesic**—We would look fairly closely at the circumstances of that particular offence.
>
> **CHAIR**—But why would you look that? Are you serious about that?
>
> **Mr Tongue**—It includes unlawful drilling, unlawful associations—
>
> **CHAIR**—Yes, but I would have thought that if I hijacked a ship or aircraft I would be automatically disqualified as a suitable person who would not be considered to be a security risk.
>
> **Mr Tongue**—The list is trying to break a large mass of people into 'green lights', 'red lights' or 'automatically disqualified'.
>
> **CHAIR**—I understand all that. But it is a pretty generous set of lights you have.
>
> **Ms Liubesic**—This is a consensus list.
>
> **CHAIR**—I am sure it is, and I beg to differ with the mob that put it together. I would have thought that if I hijacked a ship under no circumstances would I be a suitable person to go and work on a bloody wharf or rig somewhere.
>
> **Ms Liubesic**—There are also circumstances where perhaps somebody was under the influence of drugs or alcohol and tried to attempt to hijack a ship or aeroplane. The intent behind listing that particular group of offences as exclusionary is that we wanted to be able to look into their circumstances.
>
> **CHAIR**—Have you got to be convicted of these crimes?

---

22 Ms Liubesic (DOTARS), *Hansard,* 12 July 2005, p. 61

23 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005*, 7 July 2005, p. 6

Ms Liubesic—Yes.[24]

2.30 In its submission recieved after the hearing, the department indicated that:

> 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.[25]

2.31 The committee notes the 8 July regulations which do not disqualify people who have been criminally convicted of destroying or hijacking an aircraft or ship from being considered for an MSIC are fundamentally flawed. It accepts the department's undertaking to review the classifications.

Consistency in IB assessments

2.32 The flexibility provided under the disqualification and exclusionary categories also raised concerns about how the discretion will be used and the basis for those judgements.

2.33 During the inquiry calls were made for a greater transparency in how assessments of exclusionary offences would be undertaken. The Transport Workers Union stated in their submission:

> DOTARS officials have advised us that where an amber light is given discretion may be used to determine whether a demonstrable link can be made between the convictions recorded and potential terrorist activity. However, the regulations do not prescribe the manner in which discretion may be applied nor the factors that may be taken into account.[26]

2.34 This issue was of particular concern for those looking forward to the post roll-out period when it is possible that DOTARS will not be involved in the determination. Adsteam Marine Limited expressed concern as to how Issuing Bodies (IBs) (see para 2.41) would make assessments on criminal background checks:

> There is potential for employers acting as issuing bodies to impose their own character test through the vetting process.[27]

---

24 *Hansard,* 12 July 2005, p. 58

25 Submission No. 13, DOTARS, p. 13

26 Submission No. 7, Transport Workers Union, p. 5

27 Submission No. 9, Adsteam Marine Limited, p. 2

2.35 This concern as to how the vetting process will be undertaken once the roll out period is completed was also commented on by AAPMA:

> It is the unanimous view of all of the members of the working group that an independent government assessor should carry out the determination role for those who have an orange flag raised against them as part of the background-checking process. Any delegation of that determination role to issuing bodies will give rise to inconsistency in the application of policy relating to accepting or disqualifying the orange-flagged applicants. It will also give rise to forum shopping by applicants for MSICs, and delegating this role to an issuing body would surely involve a transfer of risk that is unacceptable to the government.[28]

2.36 The Australian Shipowners Association (ASA) also argued that the regulation providing IBs to assess background checks post 1 July 2006 will seriously compromise the MSIC regime. The ASA argued that ongoing Office of Transport Security (OTS) involvement in this function will bring:

> Consistency of application of the criteria for issuing an MSIC with a centralised application process – there are real concerns that unsuccessful MSIC applicants may seek to 'forum shop' around the country otherwise.

2.37 The ASA further commented that a central and consistent approach would create a greater confidence in the validity of MSICs. Further, that employers as IBs would not be placed in compromising positions whereby they need to assess employees' criminal backgrounds.[29] (The problems that may result from such access are explored in the following section – Privacy and Security Checks).

2.38 The committee shares the concerns that the discretion given to the criminal background assessments may result in different assessments being made. Without clear guidelines to make assessments, after the roll-out phase it will be extremely difficult to ensure consistent judgements across the range of IBs. Further, without guidelines it is difficult to ensure that there is an open and transparent approach which will stand scrutiny to these assessments.

Privacy and Security Checks

2.39 The background checks for applicants of the MSIC require an ASIO and AFP check, and in some cases a DIMIA background check. Within federal privacy laws, background checks of this nature must be required by legislation. The MTSA Act specifically enables regulations to be made authorising the use or disclosure of personal information as defined by the *Privacy Act 1988*. Information Privacy Principles 10 and 11 pertain to limiting the use and disclosure of personal information. Section 1(c) of Principle 10 states that:

---

28 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 27

29 Submission No. 3, Australian Shipowners Association, p. 3

> A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless use of the information for that other purpose is required or authorised by or under law.

Similarly, Section 1(d) of Principle 11 states that:

> A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless the disclosure is required or authorised by or under law.

2.40 As the background checks are a key element of the proposed system, in the absence of Government regulation privacy laws would prevent access to important information on the employees applying for MSICs. Consequently, the MSIC scheme and regulations authorise the legal disclosure of personal information of a sensitive nature to and by Commonwealth agencies to facilitate MSIC background checks. DOTARS states that:

> Under the MSIC Scheme applicants will be protected by the *Privacy Act 1988*… 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.[30]

2.41 The roll out phase of MSICs begins on 1 October 2005. During this phase the MSICs will be processed by the IBs, while the background checks will be assessed by the OTS. The 8 July draft regulations indicated that Issuing Bodies can be:

(a) a maritime industry participant;

(b) a body representing participants;

(c) a body representing employees of participants;

(d) a Commonwealth authority.

2.42 A participant may also engage an agent to issue MSICs, and that agent may apply to become an IB.[31]

2.43 The OTS assessments of the background checks will determine whether an applicant is eligible for a card. When 'roll out phase' ceases on 30 June 2006 there is some suggestion the IBs will make assessments of background checks.

2.44 During the inquiry, speculation as to who, after the initial 'roll out period', would be required to have access to information obtained during background checks

---

30 Submission No. 13, DOTARS, p. 4

31 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, p. 14

gave rise to concerns about the protection of applicants' privacy. Another issue touched on was the storage of the personal information of MSIC applicants.

Issuing Bodies' access to personal information

2.45 The uncertainty over what arrangements to assess the background checks will be put in place after the roll out period and the consequent access to applicants' background checks was a concern expressed by both those who are likely to be IBs and those representing applicants.

2.46 In its submission, the ASA noted that after the roll out period the majority of employers will retain the Issuing Body function. In the case where they do not, the consultants engaged as IBs have publicly indicated they will not be making MSIC application determinations. They have stated that determinations would remain with employers. The ASA further outlined:

> From the outset, employers have steadfastly reiterated the privacy and other difficulties that they will face receiving the criminal backgrounds of their employees from the Federal Police. There may even be conflicting corporate disclosure obligations to share holders in some situations if an employer is in possession of this information. If DOTARS (or another central government agency) cease to continue as the repository of these reports, there will be no other option but for employers to receive this information.[32]

2.47 In evidence to the committee, the Association of Australian Ports and Marine Authorities (AAPMA) stated:

> For reasons of privacy, issuing bodies do not want to know any of the details of the crimes listed on an applicant's MSIC consent form. A number of maritime industry participants—ports, stevedores and towage companies alike—have foreshadowed a willingness to take on the role of an issuing body. But, if they are exposed to the knowledge of an applicant's criminal past, after the roll-out period I think that a number of those issuing bodies will withdraw from the process.[33]

2.48 In its submission the Transport Workers Union (TWU) comments mirrored the comments of the employers.

> The TWU objects to this post roll out process due to the inevitable encroachment on privacy.[34]

2.49 The committee heard that the OTS revealed in working group discussions that the reason behind the arrangements after 1 July 2006 was budgeting constraints:

---

32 Submission No. 3, Australian Shipowners Association, p. 2

33 Ms Blackwell, *Hansard,* 12 July 2005, p. 27

34 Submission No. 7, Transport Workers Union, p. 5

> John Kilner was very specific at our last working group meeting. He said that he only had a budget of $300,000 and did not have enough money in his budget to accommodate those very specific safeguards that the entire maritime industry wanted to build into this. They were picked up for the nine-month roll-out period, from 1 October to 1 July 2006. After July 2006, the Office of Transport Security relinquishes its role of having that information on the results of background checks of up to 200,000 Australian workers and gives that back to the employers, who absolutely do not want it. They can speak for themselves. They will then have the responsibility of knowing the criminal background. The Federal Police have said that they cannot just pick out which bits; they will have an entire test of your entire criminal background and give it to your employer. The employers know that that will mean that any decisions that they make on the employment of their workers could be construed as being based on their criminal backgrounds, even if it is innocently made for other reasons. We support the employers on that.[35]

2.50 The department did not comment specifically on funding arrangements in relation to the post implementation phase. In their submission however, they made the following comments:

> 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.[36]

2.51 During the hearing, DOTARS indicated that the roll out phase will be used to assess the effectiveness of the regime:

> The commitment that the department has given to the working group is that the department will review its position with regard to background checking during the implementation phase. So no decision has been made yet as to whether all of that information will revert back to the employers as the issuing body.[37]

2.52 The committee notes that maritime industry participants would prefer the OTS to continue assessing criminal background checks post implementation of the regime. It acknowledges the reasons provided constitute serious considerations. It has concerns that the department's wait and evaluate position could be merely inaction and that after the roll out period the time lines required will be such that some options will be excluded. It is of the view that DOTARS should commence planning for the post roll out period now.

---

35 Mr Summers (MUA), *Hansard,* 12 July 2005, pp. 13-4

36 Submission No. 13, DOTARS, p. 4

37 Ms Liubesic (DOTARS), *Hansard,* 12 July 2005, p. 69

Data storage

2.53 An issue associated with devolving the responsibility of making the assessment of the background check is the securing and protecting of the data collected during the check. Regulation 6.07Q provides for the storage of data by IBs under the MSIC plan:

> An MSIC plan sets out procedures to be followed for the following purposes: …
>
> (d) the security of records in relation to applicants for MSICs.[38]

2.54 During the inquiry, concern that employers may access this background information and use it for purposes other than for which it was intended was expressed. Some information on record may not constitute a disqualification from an MSIC, but may tarnish the reputation of an employee amongst colleagues. The Australian Manufacturing Workers Union (AMWU) argued in the committee's hearing:

> I do not think any employer should have access to personal details of a person's past—for example, if he had been involved in some misdemeanour when he was young. I have personal experience with people, particularly on the waterfront, that have been through the correctional system, come out of that system, rehabilitated themselves and gone on to make a good life for themselves and their families. That can be affected if there is a scrutiny. That sort of information by some employers could be used unfairly and discriminatorily. We are very concerned about that.[39]

2.55 The TWU also expressed concerns that employment decisions could be influenced by information held by government agencies.[40]

2.56 The department informed the committee that discussions with government are currently underway to explore the possibility of having a central storage place for personal information of a sensitive nature.

2.57 The committee explored the possibility that IBs or employers could contact the agency storing information to gain access to details about an employee's former convictions, particularly those of long ago. DOTARS responded to this concern, by outlining first of all that should a central database agency be contacted for information, a simple yes or no answer will be given to relay whether a person holds a valid MSIC or is eligible for one:

> Mr Tongue—In advance of government decisions—and I will qualify that—it is not envisaged that it would be passing information back to

---

38 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, pp. 15-6

39 Mr Johnston (AMWU), *Hansard,* 12 July 2005, p. 9

40 Submission No. 7, Transport Workers Union, p. 5

> employers; it would be passing a decision back, either to us as the agency responsible or—
>
> Senator FERRIS—So the raw data would remain secure in a government agency—is that what you are saying?
>
> Mr Tongue—That is certainly one of the models that is being looked at. It is a bit hard for me because it is an issue that is still being considered.[41]

2.58 Secondly, the OTS offered that they will not have access to convictions of long ago under the spent convictions scheme. The scheme comes under Part VIIC of the *Crimes Act 1914 (Cth)*. It 'allows a person to disregard some old criminal convictions after ten years (or five years in the case of juvenile offenders) and provides protection against unauthorised use and disclosure of this information.'[42] The number of years varies according to each jurisdiction as each jurisdiction has a different spent convictions scheme.

> Senator FERRIS—If somebody has had a childhood conviction recorded against them some years ago, presumably they would have to disclose that as part of the checking mechanism. You are confirming for me that that information, which may not have been disclosed by that person in their employment, which may already be in a maritime environment, would then not be passed on to the employer; it would be held as raw data in a secure agency.
>
> Mr Tongue—If it was a childhood offence or an offence early in a person's life, it could well be that such a conviction is spent. That means that nobody sees it; we do not get access to it.[43]

2.59 The department does note in their submission however, that they have:

> Applied for and received agreement from the Privacy Commissioner and Attorney General's Department for an exclusion from the Spent Convictions Scheme for all maritime-security-relevant-offences.[44]

2.60 The committee is of the view that securing and protecting any information collected during background checks is paramount if future litigation is to be avoided. There needs to be a secure and apparent firewall between the checking and assessing body and the employer. DOTARS needs to address this perception that the information will not be secure and quarantined from other decisions.

---

41 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 62

42 The Office of the Federal Privacy Commission, *Spent Convictions,* p. 1 www.privacy.gov.au/act/convictions/index_print.html

43 *Hansard,* 12 July 2005, p. 62

44 Submission No. 13, DOTARS, p. 12

Cost Recovery

2.61 During the inquiry the committee explored the issue of cost recovery. The issue drew a number of concerns – not just in terms of who will meet the initial costs but also in relation to duplication of identity cards between the aviation and maritime industries and the validity of the costs for infrequent users.

2.62 The draft regulations set out in subdivision 6.1A.8, Regulation 6.09A provide means of cost recovery for the MSIC:

> An issuing body may recover the reasonable costs of the issue of an MSIC from the person who asks the body to issue the MSIC.[45]

2.63 The Explanatory Memorandum outlines the cost of issuing an MSIC as approximately $130 with a validity of 5 years. Costs are expected to vary between IBs based on the number of MSICs that they produce and individual IBs' cost recovery arrangements.[46] This cost comprises a security check in the vicinity of $50, and administration and production costs.

2.64 The Australian Institute of Marine and Power Engineers (AIMPE) states in its submission:

> AIMPE does not believe that this cost burden should fall on the workers being required to obtain the MSIC… The effect of the cost recovery clause appears to be to make seafarers and others pay the price of improving maritime security.[47]

2.65 During the hearing the committee heard from the AAPMA that employers are expecting to absorb the cost of the MSICs as part of the cost of doing business. The Australia Shipowners Association (ASA) however, outlined that some employers would recover MSIC costs from employees:

> There are some employers who are openly acknowledging that this is part of the overall maritime security regime. They pay for everything else. They pay for medicals and so on and so forth, so it is consistent with their operations to also pay for the application cost of an MSIC. At the other end of the spectrum, there are other employers who are looking at the recurring costs of MSICs over a period of time, which in some operations is not inconsiderable. They are exploring options for how they may or may not seek to recover that from employees.[48]

2.66 Unions are against the proposition that MSIC card holders should pay for the cards. It is argued 'that the cost of applying for and obtaining an MSIC must not in any

---

45 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, p 38

46 Explanatory Memorandum, p. 27

47 Submission No. 1, Australian Institute of Marine and Power Engineers, p. 2

48 Mr Griffett, *Hansard,* 12 July 2005, p. 42

circumstances be passed on to individual employees… in our view these costs must be recovered from employers, not individuals.'[49]

2.67 The department stated in relation to cost recovery:

> Mr Tongue—The government's position on critical infrastructure protection is that the costs of security are a cost of doing business. The only area where we have gone beyond that principle is in the area of small regional airports, where funding has been provided for a range of protective activity…there is no thought at the moment that any assistance would be provided.
>
> Senator FERRIS—So it is accepted that either the employee pays or the employer pays?
>
> Mr Tongue—That is correct.[50]

2.68 The committee acknowledges the department's clarification of the government's position. It notes that it is in accordance with the practice elsewhere in the transport industry and that industry participants can work within the framework provided and assess who will meet the costs.

Card Use

2.69 Another point of concern raised by the TWU was the potential for some truck drivers to have the need to own both a MSIC and an Aviation Security Identification Card (ASIC):

> Ms Whyte—The point we make about that is that it is a real possibility that our drivers—or their employers, the prime contractors, whoever—might have to apply and pay for a number of cards to enter a number of maritime security zones… unlike the MUA workers who are employed by P&O and go to work there every day, our drivers might go to P&O in Brisbane and then go to Patrick's in Melbourne.
>
> Senator WEBBER—So they would have to have a different card each time?
>
> Senator STERLE—And not only that, would they have to have an aviation card as well?
>
> Ms Whyte—Potentially.
>
> Senator STERLE—So the double-up in the cost could be quite astronomical for the ordinary truck driver.[51]

2.70 The issue of escalating costs for those holding ASIC and MSIC cards was addressed in the draft regulations under 6.08E:

---

49 Submission No. 8, MUA, RTBU and AMWU, p. 12

50 *Hansard,* 12 July 2005, pp. 62-3

51 *Hansard,* 12 July 2005, p. 24

> An issuing body may issue an MSIC to a person without verifying that the person has satisfied the criteria set out in subregulation 6.08C(1) if the person: (a) holds an ASIC issued under the Aviation Transport Security Regulations 2005; and (b) has an operational need for an MSIC.[52]

2.71 The regulations further elaborate that the MSIC should expire on the same day as the ASIC. The criteria set out in subregulation 6.08(1) provides for cost saving measures for the application process and background checks of an MSIC applicant who holds an ASIC. However, presumably there will still be costs associated with the production of the card.

2.72 The Committee notes the cost effectiveness of this regulation. However, while solving the problems arising from cost implications, it raises a number of additional problems.

2.73 The regime for background checks provided for applicants of an ASIC is different to that provided under the draft regulations relating the MSIC. There are no disqualifying or exclusionary provisions relating to the ASIC. Further on the committee's reading, the threshold for offences is substantially different. The ASIC regulations do not list offences that involve counterfeiting or falsification of identity documents, whereas the MSIC regulations stipulate these as exclusionary offences. The committee assumes that these thresholds differ for a reason such as different assessed risks in the two zones. Therefore, if its inclusion is based on cost considerations, the Committee has reservations about this regulation. The committee will request DOTARS to review the two systems of background checks, and if there is any difference between the two, to reconsider this regulation prior to finalising the regulations.

Infrequent users of the MSIC

2.74 Another cost concern highlighted during the inquiry was the cost to workers who may only require access to a secure maritime area once a year.

2.75 The regulations provide for a worker who may access a secure maritime area only once a year to obtain a MSIC. The draft regulations state in Division 6.1A, Regulation 6.07F:

> For this Division, a person has an operational need to hold an MSIC if his or her occupation or business interests require, or will require, him or her to have unmonitored access to a maritime security zone at least once a year.[53]

2.76 However, the AAPMA commented:

---

52 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, p. 24

53 Draft *Maritime Transport and Offshore Security Amendment Regulations 2005,* 7 July 2005, pp. 7-8

> …if I take up Senator Sterle's point, during earlier evidence, about the truck driver who comes in from the farm once a year to deliver a truckload of grain: he or she will not have an MSIC; they do not have a requirement for an MSIC. But they must be allowed to enter that maritime security zone to deliver the grain to the waiting ship. These provisions allow that person to be either escorted or continuously monitored by the use of CCTV so that business is not hampered and so that our exports can continue. There will be a range of visitors like that who will come to the port and who will not need an MSIC but who can be escorted.[54]

2.77 The committee welcomes the flexibility indicated by AAPMA in assisting infrequent users to the ports. However, it believes that this flexibility should be incorporated in the legislation to reflect the secure environment. The committee acknowledges the department's advice subsequent to the hearing that those monitoring the CCTVs will be required to have MSICs.[55] The committee is also of the view that those entering the maritime security zone (MSZ) under those provisions should be required to 'sign in' by signing a log book and displaying a form of photographic identification. Further, the 'escort' via CCTV should be undertaken on a one on one basis. The committee requests DOTARS review the regulations to accommodate these points.

Competition between Issuing Bodies

2.78 MSICs will be issued by Issuing Bodies and those bodies will have discretion as to the charge applied to the provision of the card. Charges between IBs may be cheaper as a result of a number of factors.[56] This creates a possibility for MSIC applicants to shop around for a cheaper card. Shipping Australia Limited commented:

> We believe that the proposed cost recovery model is reasonable in its general approach in that issuing bodies for MSICs, for example, can do it themselves or those involved can request others to do it for them and for those that outsource those requirements, presumably, there will be competing issuing bodies that would meet their requirements and therefore we believe that cost should be kept to a minimum.[57]

2.79 The committee notes the view that competition between issuing bodies will keep costs to a minimum.

Redundancy

2.80 The inquiry revealed a 'hidden' cost issue in the roll out of the MSIC regime. That issue is the cost associated with those who are currently working in an MSZ and

---

54 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 32

55 Submission No. 13, DOTARS, 'Answer to question 16', p. 40

56 Submission No. 13, DOTARS, 'Answer to question 9', pp. 31-33

57 Submission No. 2, Shipping Australia Limited, p. 2

will not meet the requirements to be issued with an MSIC. Apart from the human cost, if an employer cannot find suitable alternative employment, there is the potential for disqualified applicants of the MSIC to pursue redundancy benefits and unfair dismissal claims. These claims would be based on the argument that holding the MSIC was not a condition of employment. In these cases ineligible MSIC applicants could appeal to the Industrial Relations Commission or take up claims of discrimination with the Equal Opportunity Commission.

2.81 The unions argued that if an ineligible MSIC applicant has no other work available to them they should be compensated:

> we would initially be seeking compensation from the employer because the member cannot come to work anymore—it is something that is imposed on them in the middle of their working life... If the companies were able to get that compensation from the government because the government made these imposts and not the companies, that would be the companies' decision… These are unprecedented redundancies. This has not happened to anybody before, so we would be looking to what that person may have earned in the future, probably coupled with how long they had been employed.[58]

2.82 The department did not foresee the need for compensation. It argued an ineligible MSIC applicant can be granted work somewhere else within the maritime facility they are employed in.

> Ms Liubesic—If workers are ineligible to have an MSIC the onus will be on the employer to ensure that the person does not have access to a maritime security zone—so, in effect, a redeployment away from the maritime security zone.
>
> Senator O'BRIEN—And if there is no other position with that employer?
>
> Ms Liubesic—Our position is that it is a redeployment issue for the employer.[59]

2.83 The ASA noted that it would be difficult to re-deploy those workers who could not obtain an MSIC:

> For ship operators in almost all circumstances, holding a valid MSIC will constitute a condition of employment. Where an existing employee fails to obtain an MSIC, all attempts will be made to find alternative duties. This is not a redundancy per se. However, it must be said that, for a seafarer who no longer holds the requisite certification for employment, the MSIC—as opposed to being redundant to operations—it may in a great many circumstances be very difficult to find suitable alternative duties.[60]

---

58 Mr Summers (MUA), *Hansard,* 12 July 2005, pp. 17-8

59 DOTARS, *Hansard,* 12 July 2005, p. 67

60 Mr Griffett (ASA), *Hansard,* 12 July 2005, p. 41

2.84 The Customs Brokers and Forwarders Council relayed that there would be scope for members of their organisation to find work in clerical areas where an MSIC would not be required.[61] The AAPMA made similar indications:

> Let me say that none of us is looking forward to the day when one of our employees is prevented from holding an MSIC. That is going to be a frightening and terrible occasion for everybody involved. In the port environment, it may be possible in some areas to redeploy that person to a less security-sensitive area. However, we do not really operate with spare capacity any longer on the ports. I know that the port authorities will employ every means of structural adjustment possible to try and retrain that person and find them an alternative position within the maritime environment... I would like to see some government assistance, certainly, given to retrain those people that cannot hold MSICs because it is of no fault of their own... However, if that is not forthcoming then, yes, the employers—the port authorities—will be providing compensation, as Mr Summers called it.[62]

2.85 The committee notes the divergence of views on this matter and is of the view that further work on a co-operative basis needs to be done if litigation is to be avoided. It appreciates the difficulties posed for employer organisations in making any decisions about any possible redeployment or payouts until more information is available on the how many workers will be affected, and in which areas of industry.

2.86 The committee also questions whether moving an ineligible MSIC applicant to an administrative area would not also pose a security threat. There was the argument that a potential terrorist could do damage in administrative areas as well.[63]

2.87 In this context, the committee notes the AAPMA could see the benefit of continuing the consultation process, noting the achievements of the working group. 'I urge DOTARS to consider extending the life of the working group.'[64]

2.88 Although the committee notes the department's view that redeployment is a matter for the industry participants, it believes that the questions of redundancies and redeployment are matters that could usefully be explored in the working group. The committee asks DOTARS to extend the life of the working group to include the MSIC roll out period so that some assessment can be made of the employment ramifications of the regime.

---

61 *Hansard,* 12 July 2005, p. 49

62 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 36

63 *Hansard,* 12 July 2005, p. 51

64 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, p. 30

Chapter 3

Administration

Introduction

3.1 The *Maritime Transport Security Amendment Act 2005* (MTSA Act) and the associated regulations establish the MSIC regime. Yet, the success of the regime as a counter terrorist measure lies in the diligence with which the regime is followed. The enforcement of the regime with the necessary compliance checks is a critical component in that success. The committee's terms of reference recognise these aspects of the regime by requiring the examination of the adequacy of the law enforcement and oversight and compliance mechanisms and the existing checks for foreign seafarers. The committee examines issues relating to these terms of reference in this chapter.

Law Enforcement and Compliance Mechanisms

3.2 During the inquiry a number of issues emerged relating to card holder compliance and law enforcement. These issues addressed the adequacy of resources to enforce the regime and compliance with the regulations to display the card, issuing cards at short notice, compliance by foreign workers, and a need for a centralised live data base.

Inspecting facilities to enforce the MSIC regime

3.3 An adequate inspection program is critical to the MSIC regime. During the committee's hearing a number of organisations cast doubt on the Department of Transport and Regional Services' (DOTARS) capacity and expertise to check MSIC compliance in the relevant facilities.

3.4 The AAPMA questioned whether the number of Maritime Security Inspectors currently employed by DOTARS is sufficient for the task.[1]

> To come back to the number of security inspectors and people that DOTARS is employing, not a weekend goes by where we don't all see advertisements in the Australian placed by DOTARS and the Office of Transport Security for maritime specialists to come and assist them. This is a real problem that the department has faced. They simply do not have the personnel with the expertise in a maritime environment—who can basically tell their port from their starboard, who know the blunt end from the pointy end of a ship. We had a lot of people in the earlier stages from the aviation environment who really did not understand ports or how they operated….[2]

---

1 Submission No. 10, AAPMA, p. 5

2 Ms Blackwell (AAPMA), *Hansard,* 12 July 205, p. 33

3.5 The MUA, RTBU and AMWU joint submission echoed the concerns of the lack of maritime expertise in government departments:

> With the slow decline in the Australian shipping industry also comes the demise of Australia's maritime skills base… It has been reported that government departments trying to get an understanding of the complexities of the industry experienced enormous difficulties in sourcing the appropriate people because of the shortage.[3]

3.6 DOTARS outlined their regulatory responsibilities of the MSIC regime as follows:

> -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…
>
> 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 Government to explicitly regulate in this area. .[4]

3.7 The department is confident that it will be in a position to undertake these duties. Officers gave evidence to the committee indicating that the display of the MSIC would be enforced by the inspection of facilities. OTS inspection officers would visit facilities and observe whether the cards were displayed by workers in maritime security zones:

> The office currently has around 250 staff, and we have recently advertised to recruit some more. At the moment, we have 70 or 80 people in our state offices who do the compliance function. Once this system is up and going, there is a range of methods that we will employ, from individual inspectors who will go out to ports and make surprise visits through to something that we have recently done at major airports, which is flood the place with inspectors.[5]

3.8 The committee notes the concern industry participants have in the department's readiness to undertake the tasks imposed by the new legislation. It accepts the department's reassurances, particularly in relation to checking compliance of card holders displaying their cards.

---

3 Submission No. 8, MUA, RTBU, AMWU, p. 14

4 Submission No. 13, DOTARS, p. 5

5 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 65

3.9 The importance of the card and its clear visibility is evident in the regulatory framework which imposes significant penalties on a card holder for failure to properly display the MSIC.

Display of the MSIC

3.10 The 8 July draft regulations outline the requirements for displaying the MSIC correctly. Draft regulation 6.07E states that the MSIC is defined as being 'properly displayed' if it is attached to a person's outer clothing, above waist height, at the front or side of the body; and with the whole front of the MSIC clearly visible.[6] In subdivision 6.1A.2, regulation 6.07J, the penalties for not properly displaying a valid MSIC are as follows:

> (c) for a first offence – 5 penalty units; or
>
> (d) for a second offence within 2 years of an offence – 10 penalty units; or
>
> (e) for a third or subsequent offence within 2 years of an offence – 20 penalty units[7]

Inequitable penalties for incorrectly displaying the MSIC?

3.11 Some organisations argued that the penalties imposed for not displaying the MSIC correctly were too harsh in comparison to penalties for other breaches of maritime security.

3.12 The Maritime Union of Australia (MUA) raised these concerns. Mr Summers told of a vessel that had been inspected and found to have deplorable working conditions. When inspectors of the MUA attempted to board the vessel to continue investigations, the captain had put the ship onto a security level 2 and raised the gangway, prohibiting the inspectors from boarding the vessel.

> This was a clear breach of maritime security. It had nothing to do with maritime security at all and it really had everything to do with him protecting prying eyes from seeing what deplorable conditions he was making his crews work under. We made a lot of noise about this, but still the captain… got away completely unpunished and so did the company.[8]

3.13 The MUA argues that it is inequitable to allow a breach of that magnitude go unpunished, yet expect employees to be penalised for incorrectly displaying their cards:

> So that goes unpunished and yet there are conditions and provisions inside these regulations—in the first draft—that would take away a person's card

---

6 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 7

7 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 11

8 Mr Summers (MUA), *Hansard,* 12 July 2005, p. 19

> if they did not show it properly three times in a row. Now there is a penalty of up to 20 penalty points, and I think they are $110 each. So that is quite a substantial fine for simply not showing your card correctly. In a work site you may not always be aware that it has tucked under, flicked over or fallen off.[9]

3.14 The committee notes the MUA's concerns and recognises the security issues raised in the example provided to the committee. However, the committee does not consider that difficulties with other aspects of maritime security are a justification for downgrading the need to enforce compliance to clearly display the MSIC. The penalty provisions of the regulations provide a mechanism to enforce that compliance.

3.15 The committee is concerned however, to ensure that compliance with the regulations does not constitute an occupational health and safety issue.

OH&S standards for display of the MSIC

3.16 A representative of the MUA commented there has already been recognition within industry of the potential safety hazard in display of the MSIC:

> It is a very dangerous implementation, because if you are working on top of a stack of containers that are 10 or 15 high and it flicks off and falls down the bottom, you are not going to unstack the whole ship to get to your security card, so there is that. I know that the employers are talking about introducing some other mechanisms in their workers overalls to slide [the MSIC] in so it is not hanging loose. You certainly would not work on a ship or an offshore platform with a noose around your neck, because it is absolutely dangerous and could cause catastrophic events. So it has to be above your waist, below your shoulder and showing out all the time. For the first time, contravention—not having it exactly the right way or if it is flicked around—brings a monetary penalty for those who are supposed to be involved.[10]

3.17 The department recognised the potential choking hazard that an MSIC hung around the neck could be:

> 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?
>
> Ms Liubesic—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

9 Mr Summers (MUA), *Hansard,* 12 July 2005, p. 19

10 Mr Summers (MUA), *Hansard,* 12 July 2005, p. 20

> have an MSIC dangling on the end of a lanyard which could get caught on machinery, that is what that clause is referring to.[11]

3.18 Draft regulation 6.07M provides an exemption to the display of the card. However, it does not exempt employees from obtaining the card and undergoing the necessary background checks.[12]

3.19 In addition, due to the nature of maritime work, there is potential for the card to become lost or inadvertently shipped to another port. Regulation 6.08R provides for a MSIC holder who becomes aware their card has been lost, stolen or destroyed to make a statutory declaration within 7 days. In the case where it is stolen, the MSIC holder is to give the IB a copy of the police report within 7 days of the theft.[13]

3.20 The committee appreciates the need to balance the operational requirements and safety concerns of those required to display the MSIC with the security requirements. It is of the view that these issues have been provided for in the draft regulations so that compliance can be properly monitored.

Issuing MSICs at short notice

3.21 Another issue raised during the hearing that was of concern to the committee was the potential for applicants to experience delays in employment while waiting for an MSIC application to be processed:

3.22 At the hearing the MUA outlined the difficulties:

> The nature of the industry is such that you can get a call in the middle of the night asking you to be on a plane at six o'clock in the morning. We have to provide them with a card ready to go, rather than say, 'You have to be picked up in three months time so you had better start the process of getting a background check.'[14]

3.23 However, the unions acknowledged that DOTARS took these issues into consideration by allowing unions to become Issuing Bodies (IBs).

> The union indicated very early in the piece that we wanted to be an issuing body. Essentially, for the seamen and the seafarers of the Maritime Union of Australia and I understand some of the casual workers in other areas, if we are an issuing body that would provide our members with the opportunity to be ready to be employed immediately. If they had to wait for

11 *Hansard,* 12 July 2005, pp. 65-6

12 *Hansard,* 12 July 2005, p. 66

13 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, pp. 32-3

14 Mr Summers (MUA), *Hansard,* 12 July 2005, p. 12

> criminal background checks and if they had to wait to get an employer before they could start that process, then it could impede the industry.[15]

3.24 Draft regulation 6.07O(1)(c) provides 'a body representing employees or participants' may apply for authorisation as an IB.[16]

3.25 The committee welcomes this cooperation and acknowledges the unions' work on behalf of their members. It hopes that accommodating such concerns will improve compliance with the requirements placed on workers.

3.26 An associated matter raised during the inquiry was the requirements that might be placed on foreign workers who are employed in the maritime industry.

Skills base and foreign workers

3.27 In some cases imported skilled labour is required in the maritime industry. The AMWU raised the issue of 'guest labour' to Australia, and if these foreign workers would undergo security checks:

> Guest labour… is currently being utilised in this country—coming from South Africa, Asia… Korea and even Hungary. Because we have not yet come across this added security arrangement, the only check that is available to contractors and labour hire people is basically an induction of the facility. So if labour hire people went offshore with a contractor they would be subject to the induction of that facility—that is all. And they would probably be under the supervision of the host company, the major contractor. There would be no real security check. I do not know how you would check on the security of 50 boilermakers, welders and riggers coming from, say, Malaysia or Indonesia to work on the North West Shelf or to work at a facility in Perth.[17]

3.28 The committee queried if practical measures had been put into place to ensure these foreign workers are provided with MSICs if required. [18] The department responded that foreign workers are still required to hold an MSIC. If a foreign worker could not obtain an MSIC they would have to be escorted or continuously monitored in their duties. DOTARS has begun discussions with DIMIA in regard to educating foreign workers in advance about MSIC requirements before they arrive in Australia with employment contracts.[19]

---

15 Mr Summers (MUA), *Hansard,* 12 July 2005, p. 6

16 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 14

17 Mr Johnston (AMWU), *Hansard,* 12 July 2005, p. 26

18 *Hansard,* 12 July 2005, p. 78

19 *Hansard,* 12 July 2005, pp. 78-9

3.29 The committee notes the practical measures taken by DOTARS to ensure that 'guest workers' are aware of the requirements. It also notes the provisions of draft regulation 6.07H relating to the authentication of certain foreign documents. However, the critical issues are how are the security checks going to be applied and by whom. The offences listed as maritime security relevant offences relate to the Australian context. While the committee has no argument with this, it does have concerns as to how this translates to the law in other countries and the significance this has for those coming to work in Australian maritime facilities. The department indicates in relation to foreign seafarers that background checks are 'limited by the laws of those countries'[20]. The committee asks DOTARS to consider these statements in the context of 'guest labour' and review these issues prior to finalising the regulations.

Live background checks of the MSIC

3.30 Issues relating to security checks did not just relate to foreign workers. The practical aspects of the security checks were also questioned during the inquiry.

3.31 Given the MSIC is valid for 5 years, queries about the reliability of the security checks during that term were voiced. The AAPMA noted that:

> During our working group deliberations we have had the benefit of having ASIO and AFP representatives present. ASIO have checks that are live and ongoing so that once you sign the consent form ASIO can continue to check your background continually on a live database. Unfortunately, it seems that the AFP database is not similarly live. The checks that the AFP carries out, it seems, both within its own database and then in cooperation with all the various state police databases, are static as of the date that the applicant signs that form. So, if an MSIC holder later on has a conviction recorded against them, we are not going to know about that until their MSIC is renewed five years later. I would suggest that that too is an unacceptable risk that we do not wish to take. I appreciate that coordinating all of the police databases around the states and the Commonwealth is a huge task. I have heard a rumour that work is commencing on a program but I am not sure of the details of that... I commend that as an initiative in the security environment in which we are now working.[21]

3.32 The ASA commented that a centralised approach to the MSIC regime would allow for the development of a central database of valid MSICs:

> This would enable basic checking of validity by employers for relief crews on ships and sub-contracting truck drivers for port facilities.[22]

3.33 DOTARS speculated on the development of a centralised data base that was routinely updated, but was not able to give any confirmation:

---

20 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 71

21 Ms Blackwell (AAPMA), *Hansard,* 12 July 2005, pp. 27-8

22 Submission No. 3, Australian Shipowners Association, p. 3

> …given that background checking as a security device is growing across the economy, …is whether we might not be able to build a more efficient system in the Attorney-General's portfolio. The government has made no final decisions yet; it is still looking at the issue. But the idea is that there would be a central agency that coordinates between AFP, ASIO and the immigration department with respect to background checking. In advance of government decisions about how that organisation might be built, it is a bit hard for me to say that there would definitely be a live list of people, because the government may choose to build the agency up in a different way.[23]

3.34 The committee notes that the draft regulations provide a means by which background checks can be undertaken during the term of the MSIC. Regulation 6.08C(6) states:

> An issuing body may issue an MSIC subject to a condition, but must notify the holder in writing what the condition is.
>
> *Example*
>
> A condition that background checking of the holder is carried out more frequently than required by these Regulations.[24]

3.35 The committee notes that these provisions may be useful at the outset in providing an applicant with a card but does not address the issue – that is flagging when a card holder has been convicted of an "amber light" maritime security relevant offence and needs to be further monitored.

3.36 The AAPMA argued in their submission that the process to allow for live background checking should be a matter of priority:

> 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.[25]

3.37 The committee notes the concerns and asks the government to take the committee's evidence into account and to give priority to such work.

Monitoring Non-MSIC Holders

3.38 The draft regulations acknowledge that there will be some persons ineligible for a MSIC but who will on occasions access a maritime security zone (MSZ). Draft regulation 6.07 establishes an offence if such persons or 'visitors' are not escorted or continuously monitored when in a MSZ.

---

23 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 61

24 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 23

25 Submission No. 10, AAPMA, p. 3

3.39 The committee inquired of the department how non-MSIC holders would be monitored when in secure maritime areas:

> Senator O'BRIEN—Concern has been expressed to this committee about proposed arrangements that will permit non-maritime security identification cardholders access to maritime security areas. Am I correct in understanding that visitors will be permitted to access secure areas without a physical escort provided they are continuously monitored?
>
> Ms Liubesic—Yes, that is right.
>
> Senator O'BRIEN—By closed-circuit television, I presume?
>
> Ms Liubesic—By either closed-circuit television on a continuous basis—so not segments of time—or under the escort of a person who is an MSIC holder.[26]

3.40 During the hearing the unions queried whether those monitoring non-MSIC holders via CCTV would be required to hold MSICs. The committee followed this query through to the department:

> Senator O'BRIEN—Will the person charged with the responsibility for continuous monitoring be required to hold an MSIC?
>
> Ms Liubesic—It is an issue that we are currently looking at. This has been raised by our working group, and we are looking at that issue at the moment.[27]

3.41 The department has since clarified this evidence in their submission. Regulation 6.07J(2) specifies the requirements of an escort in a MSZ is to hold a valid MSIC:

> 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.[28]

3.42 The committee was not able to establish an estimate as to how many people will require monitored access to MSZ. The department informed the committee that that they do not have an estimate.[29] However, as discussed in paragraph 2.77, the committee is of the view that more rigorous requirements need to be incorporated in the regulations to ensure the secure environment.

3.43 The committee notes that escorted visitor status does not apply to personnel required to access MSZ in the case of emergencies.

---

26 *Hansard,* 12 July 2005, p. 65

27 *Hansard,* 12 July 2005, p. 65

28 Submission No. 13, DOTARS, 'Answer to Question 16', p. 40

29 *Hansard,* 12 July 2005, p. 92

Enforcing the MSIC in circumstances involving an emergency

3.44 Regulation 6.07N allows ambulance, rescue or fire service officers to access maritime security zones in the case of an emergency.

3.45 The AAPMA argue that greater provision is needed for emergencies such as oil spills and 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… 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.[30]

3.46 DOTARS responded by outlining that the exemption provisions in the regulations are for occupational, health and safety reasons (see para 3.17). The exemption principles are not provided for emergency personnel. Access for emergency personnel is provided for in Regulations 6.07J(2)(b) and 6.07(N). A departmental officer elaborated:

> 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.[31]

3.47 However, the AAPMA noted in their submission that DOTARS had advised them, that to allow MSZ access to a wider range of emergency personnel, 'the re-wording of the relevant sections requires legal advice with likely policy implications and we understand that work is progressing on this front.'[32]

3.48 The department further clarified the position in their submission by indicating that arrangements have been made for emergency personnel in the case of environmental emergencies:

> 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.[33]

---

30 Submission No. 10, AAPMA, p. 4

31 Ms Luibesic (DOTARS), *Hansard,* 12 July 2005, p. 66

32 Submission No. 10, AAPMA, p. 4

33 Submission No. 13, DOTARS, 'Answer to Question 6', p. 29

3.49 The committee notes the need for speedy access to a MSZ in the case of an emergency and welcomes the exemptions that have been established for emergency personnel. However, the committee believes that such access should be balanced with the long terms requirements to ensure a secure environment. Therefore, compliance and monitoring responsibilities should not be compromised.

Boarding a vessel as part of a recreational activity

3.50 Given the requirements on access by emergency personnel, the committee was interested in draft regulation 6.07K which provides for a person who has been given a MSIC disqualifying notice to enter a MSZ if the person:

> is a visitor to a zone for the purpose of boarding or leaving a vessel as part of a recreational activity.[34]

3.51 The committee explored the matter with the AAPMA, citing the port of Hobart as an example where small sailing vessels pull along side working wharves in a port:

> Senator O'BRIEN—The point I am making is that the terminology says 'boarding or leaving a vessel'. So, if there is any sort of vessel moored alongside, there is an exemption under the regulation for a person who would otherwise be excluded, provided they say that they intend to visit the zone to board or leave that vessel for recreational purposes.
>
> Ms Blackwell—...It was there to cover people who board a cruise vessel. When you board a cruise vessel, you go through the cleared zones, a bit like you do when you are in an airport. But I take your point. I think there could be tighter wording… I am not putting words into DOTARS' mouth, but perhaps they were thinking that around cruise vessels you have this maritime exclusionary zone and you are not supposed to broach that. There are vessels that are supposed to be on the water, monitoring all of that. But it could be tighter, Senator, I agree. It could be reworded.[35]

3.52 The committee agrees that the wording needs to be tighter and asks the department to review the wording of draft regulation 6.07K prior to finalising the regulations.

Foreign Seafarers

3.53 The final component of the committee's terms of reference required the committee to examine the adequacy of the existing checks for foreign seafarers.

---

34 Draft Maritime Transport and Offshore Security Amendment Regulations 2005*,* 7 July 2005, p. 12

35 *Hansard,* 12 July 2005, p. 35

3.54 The department informed the committee that over 200,000 foreign seafarers enter Australian ports each year.[36] There was concern that Australian seafarers are required to undergo security checks before they can work on Australian maritime facilities including ports, while foreign seafarers were receiving no background checks at all.

3.55 The unions' joint submission outlined these concerns:

> Where the MSIC will see a high level of background checking on all Australian seafarers from our top law and intelligence bodies the same is impossible for foreign nationals.[37]

3.56 International Labor Organisation (ILO) Convention 185 found favour with those who were concerned that the current MTSA Act does not allow for background checking of foreign crews.[38] ILO Convention No. 185 provides an international identification system available to governments, ship owners and seafarers. The identity document for seafarers uses a 'biometric template' to adapt two fingerprints of a seafarer into a standardised 2-D barcode on the Seafarers' Identity Document (SID).[39]

3.57 The department confirmed that while MSICs will be required for foreign seafarers on Australian flagged ships, seafarers on foreign flagged vessels will not be required to hold an MSIC.

3.58 However, foreign seafarers entering Australia are subject to checks. The Australian Customs Service outlined the current security checks of foreign vessels:

> Customs risk assesses every commercial vessel in advance of its arrival in Australia. The assessment takes into account government information and intelligence in relation to terrorism.
>
> Crew details including name, date of birth and passport information are obtained in advance of arrival. The details of every crew member are entered into a Customs system that is checked against the Passenger Analysis, Clearance and Evaluation (PACE) system. This includes the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) Alert List and alerts placed by other agencies, including national security agencies.[40]

3.59 DOTARS further indicated:

---

36 *Hansard,* 12 July 2005, p. 71

37 Submission No. 8, MUA, RTBU, AMWU, p. 14

38 Submission No. 8, MUA, RTBU, AMWU, p. 14

39 'New ratification opens the way for ILO Convention on seafarers' ID card', *International Labor Organization,* 17 August 2004, p. 1

40 Submission No. 11, *Australian Customs Service,* p. 2

> Foreign seafarers is a complex area, and we have been doing some work with the immigration department to look at the possibility of bringing in an enhanced regime for foreign seafarers that would include some form of visa requirement... Involving a background checking regime that would apply if you were applying for a tourist visa or other visa to enter Australia, which would enhance the current background checking regime. Our ability to background check to the same standard as we are doing in Australia in other countries is limited by the laws of those countries. We are certainly aware of the need to enhance that area, and we are working with immigration to do it.[41]

3.60 The department acknowledged the difficulties in enforcing any sort of regulations on a foreign flagged ship, and especially a vessel with flags of convenience.

Flags of convenience and the Coastal Permit System

3.61 Vessels with flags of convenience and vessels holding coastal permits frequent the Australian coast. A ship that flies a flag of convenience flies the flag of a country other than the country of ownership. It is suggested that these merchant vessels are registered this way for the purpose of reducing operating costs or avoiding government regulations.[42] DOTARS does not recognise the term 'flag of convenience' as an officially recognised category of vessels.[43]

3.62 The coastal permit system allows for the issue of Single Voyage Permits (SVPs) and Continuing Voyage Permits (CVPs). SVPs are issued for a single voyage between designated ports for the carriage of specified passengers or goods. CVPs are issued for a period of up to three months and allow a vessel to carry specified cargo between specified ports for that period. The permits are kept to a low cost; cargo SVPs are $200.00 and CVPs are $400.00.

3.63 The joint union submission made the following comments on the current system:

> While unions support the coastal voyage permit system we do not support the abuses under them. … The most obvious prospect for potential terrorists to breach our maritime security is by using flags of convenience shipping on government permits to replace entire trades on our coast at the expense of Australian shipping.[44]

3.64 The committee questioned the department about the matter of foreign vessels using flags of convenience:

---

41 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 71

42 Global Forum Policy, 'A Brief Guide to Flags of Convenience,' International Transport Workers' Federation, p. 1, www.globalpolicy.org./nations/flags/guide.htm

43 Submission No. 13, DOTARS, 'Answer to Question 12', p. 36

44 Submission No. 8, MUA, RTBU, AMWU, p. 14

> Senator O'BRIEN—But, even though they are operating under the flag of another nation, when they are in our ports they are under our law, aren't they?
>
> Mr Tongue—They have to comply with Australian law, but they are protected a bit because of their flag status. There are things we can do on Australian ships that we cannot do on foreign flagged ships.
>
> Senator O'BRIEN—Are you telling us that we cannot require a foreign flagged vessel not to abuse a provision of our law while it is in our port?
>
> Mr Tongue—I am saying that it is very difficult for us to prove that a foreign flagged vessel is abusing security requirements without going through a process that involves contacting the flag state first…
>
> It is easy to contact some of the flag states; we have 24-hour contact details. But some of the flag states, frankly, are pretty hard to get to.[45]

3.65 In their submission, the department further clarified the security arrangements for foreign flagged ships:

> 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.[46]

3.66 The committee notes that while the MSIC regime does not enhance the security checks of foreign seafarers, these seafarers are none the less required to abide by the principles of the regime. Access to MSZ will be on the same basis as 'visitors' access.

3.67 The committee is of the view that the government should refer the matter of the introduction of physical screening of persons who enter maritime security zones, including holders and non-holders of MSICs, to the working group for consideration.

3.68 The committee also notes the results of an internal audit report of the coastal shipping permit system conducted in June and August 2004. This review was initiated by DOTARS when permit processing responsibilities were handed over to the OTS:

> 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 licenses, changes in record management practices and as part of a broader rewrite of the Coasting Trade Regulations. These amendments are close to finalisation.[47]

---

45 *Hansard,* 12 July 2005, pp. 68-9

46 Submission No. 13, DOTARS, p. 6

47 Submission No. 13, DOTARS, 'Answer to Question 11', p. 35

Other Matters

Container Inspections and high consequence dangerous goods

3.69 During the inquiry, the Australian Workers' Union (AWU) highlighted another aspect of maritime security that it considered a risk, the threat posed by shipping containers:

> There are no physical checks at all performed on the "empties" and they are only presumed to be empty. This provides a clear portal for terrorist activities and the examples stated internationally is the opportunity for a dirty bomb to be planted in one of these empties, tracked through a major city and detonated at precise location.[48]

3.70 Further, the unions' joint submission made a call for the government to restrict the carriage of high consequence dangerous goods onboard flag of convenience foreign ships.[49]

3.71 The department responded that container inspections are primarily the responsibility of Customs:

> We have certainly been working with the Australian Customs Service, which is the responsible agency, to look at a range of supply chain and container security initiatives.[50]

3.72 The committee notes that these issues fall outside its terms of reference. Yet they are matters that warrant government consideration.

48 Submission No. 12, The Australian Workers' Union, p. 16

49 Submission No. 8, MUA, RTBU, AMWU, p. 16

50 Mr Tongue (DOTARS), *Hansard,* 12 July 2005, p. 72

Chapter 4

Conclusions and Recommendation

4.1 The committee, in undertaking its inquiry into the regulatory framework to be implemented and enforced by the Department of Transport and Regional Services (DOTARS), reviewed the *Maritime Transport Security Amendment Act 2005* and the draft regulations made under that Act. These draft regulations were the Maritime Transport and Offshore Security Amendment Regulations 2005 (dated 7 July 2005) and the Maritime Transport Security Amendment Regulations 2005 (dated 4 July 2005). The focus of the committee's work was on the set of regulations which provided the details of the maritime security identification card (MSIC) – the Maritime Transport and Offshore Security Amendment Regulations 2005 (the regulations).

4.2 Although the committee was able to satisfy a number of concerns it had with aspects of the regulations there are a number of other matters that the committee has requested DOTARS review in the draft regulations prior to gazettal. These matters include:

- the types of crime included in the exclusionary offences category for maritime security relevant offences;
- draft regulation 6.08E and the potential difference in the security checks between ASICs and MSICs;
- access provided to visitors and infrequent users of cards being monitored subject to the committee's proposed 'logging in procedure';
- the wording of draft regulation 6.07K relating to access for individuals who have a MSIC disqualifying notice;
- the security checking requirements for skilled foreign workers.

Recommendation

4.3 The committee recommends that, prior to the gazettal of the Maritime Transport and Offshore Security Amendment Regulations 2005, DOTARS review the regulations to address the committee's concerns as outlined in this report.

4.4 In addition to matters directly stemming from the draft regulations the committee has identified a number of other concerns within its terms of reference. These concerns primarily relate to privacy issues and the adequacy of the consultation mechanisms.

4.5 The committee concludes that DOTARS needs to commence work now on the post roll out phase so that the privacy concerns of both employers and employee representative bodies are addressed as soon as possible. Such work needs to address

the perception that there is not a secure and apparent firewall between the checking and assessing body and the employer.

4.6 Further, the committee concludes that guidelines to assist assessments of security checks are required for the post roll out period.

4.7 Finally, the committee draws conclusions as to the adequacy of the consultation mechanisms. In Chapter 2 the committee notes the confusion arising out of changes to the regulations relating to maritime security relevant offences is regrettable and may have been avoided if the consultation process had not been truncated. The committee notes that since its hearing the department has invited further feedback from the Working Group:

> 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.[1]

4.8 The committee welcomes this initiative. It also asks DOTARS to extend the term of the working group into the roll out period so that some assessment can be made of employment ramifications of the MSIC regime.

4.9 In conclusion, the committee accepts that DOTARS had a difficult task in meeting its responsibilities in providing the roll out of enhanced security measures for Australia's maritime industries. It commends the department for the work they have done. Nonetheless it reminds the department and its officers that they are, through their minister, answerable to the Parliament. When the Senate charges this committee with task of examining their work, they should assist the committee in that task and not proceed as if the inquiry was not being conducted. To do so indicates a disregard of the Senate and of this committee's work.

Senator the Hon. Bill Heffernan
Chair

1 Submission No. 13, DOTARS, 'Answer to Question 14', p. 38

ADDITIONAL COMMENTS BY LABOR SENATORS

Summary

Labor Senators support the implementation of a Maritime Security Identity Card (MSIC) regime.

Labor Senators strongly endorse the recommendation that the Department of Transport and Regional Services review the draft Maritime Transport and Offshore Security Amendment Regulations 2005 (the draft regulations) to positively address the many concerns expressed by this committee.

Comments

Labor Senators draw particular attention to the following issues:

Inspector of Transport Security

Labor Senators note that the Inspector of Transport Security has played no role in the development of the draft regulations despite the previous Minister for Transport and Regional Services claiming the appointee would examine "systemic transport security weaknesses to ensure security vulnerabilities are identified and addressed."

It is clear to Labor Senators that the absence of a maritime identification card regime constitutes a transport security weakness.

The Inspector of Transport Security should have been involved in the task of developing the MSIC regime.

Mr Bill Ellis, the "acting" Inspector of Transport Security describes his appointment as follows:

> My understanding is that I am appointed to a sort of panel position, where the inspector is the head of the office and other people would be appointed to a panel—of experts, or whatever—should the need arise to handle particular investigations.[1]

It is clear from Mr Ellis description that he does not consider himself to be acting in the position of Inspector of Transport Security.

In our view, it is disingenuous of the Department of Transport and Regional Services to describe him as such.

---

1 *Hansard,* 12 July 2005 p.1

Timing

Labor Senators regret the government's decision to delay the release of 'final' draft regulations to members of the industry working group and the committee until 8 July 2005 which gave witnesses and committee members just one working day to consider the amendment draft regulations before the hearing.

As noted in the report, the manner in which the amended 'final' draft regulations were circulated to working group casts doubt over the adequacy of the consultative process.

The announced gazettal timetable (21 July 2005) reveals an unhealthy disregard for the role of the Senate and this committee in particular.

Working group

Subject to the willing participation of working group members, Labor Senators believe the life of the working group should be extended through the roll-out phase to 1 July 2006.

Criminality

The report notes the evidence that draft table 6.07C in the draft regulations does not reflect the working group agreement on the level of criminality that would constitute the disqualification of an MSIC application. It also notes the government decided to amend earlier draft regulations so the final draft did not reflect the working group consensus. Labor Senators consider this decision regrettable.

While reassured that Part IIA of the *Crimes Act 1914* does not fall within the meaning of Part II contained in draft table 6.07C in the draft regulations, Labor Senators are concerned about the inclusion of the whole Part II, particularly sections 28 and 29.

Labor Senators are not satisfied that provisions related to interfering with political liberty and property offences necessarily constitute maritime security related offences.

This matter was raised during the hearing:

> Senator O'BRIEN— …What is the relevance of section 28 to maritime security? Can you explain that to me, please?
>
> Ms Liubesic—It was because there were a number of other categories in that part. That is why the whole part appears in the crimes list.
>
> Senator O'BRIEN—If the regulation had said 'part II, except sections 28 and 29', for example, that would equally cover what you intended to cover?
>
> Ms Liubesic—That is right.
>
> Senator O'BRIEN—So it could be a drafting error.

> Ms Liubesic—Yes.
>
> Senator O'BRIEN—What about 29? Why is that in there?
>
> Ms Liubesic—Again, it is the same sort of issue where the part was relevant to what we were trying to do, so we just included the entire part.[2]

Labor Senators remain dissatisfied with the department's response and urge the government to reconsider the inclusion of these offences in draft table 6.07C for reasons of convenience or, worse, drafting error.

We draw the government's attention to the intended lax operation of draft regulation 6.07K which would, on the face of it, permit persons convicted of disqualifying offences, including supplying in weapons of mass destruction, access to maritime security zones when engaged in a "recreational activity".

Labor Senators are not satisfied by the government's assurance that such persons would need to be escorted to gain access. Such persons should not have access to maritime security zones under any circumstances.

Post roll-out phase

Labor Senators share the concerns expressed by witnesses that the planned devolution of critical responsibilities, including assessment, to issuing bodies post-1 July 2006 has the potential to compromise the privacy of MSIC applicants and the overall integrity of the MSIC regime.

We urge the government to put national security interests ahead of narrow budgetary concerns and reconsider its decision to devolve critical responsibilities to issuing bodies from 1 July next year.

Cost recovery

Labor Senators are not satisfied the government has adequately addressed concerns about cost recovery.

The committee heard varying cost estimates and suggestions in relation to where the cost burden associated with obtaining a MSIC might fall.

Labor Senators believe the matter of cost recovery should be referred to the working group for further discussion.

Temporary access

2 *Hansard,* 12 July 2005 p.55

Labor Senators are deeply concerned by the government's intention to permit access to maritime security zones by non-MSIC-holders subject to little more than closed circuit television surveillance.

While welcoming the committee's recommended strengthening of the access regime through a 'sign in' system and one to one surveillance, Labor Senators believe no cogent argument has been presented for the proposed open access to maritime security zones.

We believe that access by non-MSIC-holders has the potential to degrade security and undermine the integrity of the strengthened maritime security regime.

Labor Senators urge the government not to replicate in a maritime context the airside access regime currently in place at airports and under external review due to identified deficiencies.

We urge the government to strengthen the proposed access regime by developing new regulations in consultation with members of the working group.

Foreign seafarers

Labor Senators note that foreign seafarers are not required to obtain a MSIC.

Nor does the proposed regime enhance security checks on foreign seafarers.

The joint unions' submission identifies poor screening of foreign seafarers as a weakness in Australia's maritime security.

It is a matter of regret the government has failed to address improved screening of foreign seafarers alongside the improved screening of Australian seafarers and other maritime and transport workers.

Labor Senators urged the government to address this anomaly in consultation with members of the working group.

Coastal permit system

Labor Senators are concerned about the integrity of the coastal permit system and the potential impact on maritime security arising from its abuse.

We note that an audit of the coastal permit system has identified manifest inadequacies in its administration.

Labor Senators urge the government to release the audit report and provide the committee with details of changes to procedures already implemented and proposed to be implemented through revised regulations governing coastal trading.

Abuse of maritime security

Labor Senators note evidence to the inquiry that some ships masters have abused the maritime security regime to achieve industrial objectives.

We urge the government to take action against maritime industry members who exploit security measures to achieve non-security-related objectives.

Container inspections and transport of high consequence dangerous goods

Labor Senators note the finding of the report that concerns over inadequate screening of containers transhipped through Australian ports and the carriage of high consequence dangerous goods by flag of convenience ships warrant government consideration.

We believe such glaring deficiencies in Australia's maritime security – identified in submissions to this inquiry – must be addressed as a matter of priority.

Senator Anne McEwen (ALP, South Australia)

Senator Glenn Sterle (ALP, Western Australia)

Senator Kerry O'Brien (ALP, Tasmania)

Senator Ruth Webber (ALP, Western Australia)

Appendix 1

List of Submissions

1.	Australian Institute of Marine and Power Engineers
2.	Shipping Australia Limited
3.	Australian Shipowners Association
4.	CONFIDENTIAL
5.	Australian Manufacturing Workers Union
6.	CONFIDENTIAL
7.	Transport Workers Union
7A	Transport Workers Union
8.	Maritime Union of Australia (MUA) Rail, Tram and Bus Union (RTBU) Australian Manufacturing Workers Union (AMWU)
9.	Adsteam Marine Limited
10.	The Association of Australian Ports and Marine Authorities Inc.
11.	Australian Customs Service
12.	The Australian Workers' Union (AWU)
13.	Department of Transport and Regional Services
14.	NSW Government

Appendix 2

Witnesses who appeared before the Committee at the Public Hearings

Tuesday, 12 July 2005
Parliament House, Canberra

Inspector of Transport Security
Mr William Ellis

Maritime Union of Australia
Mr Dean Summers, National Officer

Transport Workers Union
Ms Danni Whyte, Policy Development Officer

Australian Manufacturing Workers Union
Mr Patrick Johnston, National Organiser

Association of Australian Ports and Marine Authorities Inc.
Ms Susan Blackwell, Executive Officer

Australian Shipowners Association
Mr Trevor Griffett, Director – Canberra

Customs Brokers and Forwarders Council of Australia
Mr Stephen Morris, Executive Director

Department of Transport and Regional Services
Mr Michael Mrdak, Deputy Secretary
Mr Andrew Tongue, Executive Director, Office of Transport Security
Mr Ross Hallinan, Acting General Manager, Maritime Security
Ms Patricia Georgee, Section Head, Maritime Branch
Ms Patricia Liubesic, Section Head, Maritime Security Identity Team, Office of Transport Security

Appendix 3

Maritime Transport and Offshore Security Amendment Regulations 2005

Maritime Transport and Offshore Security Amendment Regulations 2005 (No.)[1]

Select Legislative Instrument 2005 No.

I, PHILIP MICHAEL JEFFERY, Governor-General of the Commonwealth of Australia, acting with the advice of the Federal Executive Council, make the following Regulations under the *Maritime Transport and Offshore Security Act 2003*.

Dated 2005

Governor-General

By His Excellency's Command

[DRAFT ONLY – NOT FOR SIGNATURE]
Minister for Transport and Regional Services

DRAFT ONLY

1 Name of Regulations

These Regulations are the *Maritime Transport and Offshore Security Amendment Regulations 2005 (No.)*.

2 Commencement

These Regulations commence on the day after they are registered.

3 Amendment of *Maritime Transport and Offshore Security Regulations 2003*

Schedule 1 amends the *Maritime Transport and Offshore Security Regulations 2003*.

Schedule 1 Amendments

(regulation 3)

[1] After regulation 3.10

insert

3.12 Operator to tell Secretary about issuing body for MSICs

(1) No later than 30 June 2006, a port operator, port facility operator or port service provider must give the Secretary the following information in writing:

(a) if the operator is not an issuing body, the identity of the person who will issue MSICs for the operator;

(b) whether the operator will issue temporary MSICs and, if not, the identity of the person who will issue temporary MSICs for the operator.

(2) The operator must notify the Secretary within 7 days if any information given for subregulation (1) is no longer correct.

[2] After regulation 5.10

insert

5.12 Operator to tell Secretary about issuing body for MSICs

(1) No later than 30 June 2006, an offshore facility operator must give the Secretary the following information in writing:

(a) if the operator is not an issuing body, the identity of the person who will issue MSICs for the operator;

(b) whether the operator will issue temporary MSICs and, if not, the identity of the person who will issue temporary MSICs for the operator.

(2) The operator must notify the Secretary within 7 days if any information given for subregulation (1) is no longer correct.

[3] Paragraph 5A.85 (1) (a)

substitute

(a) the boundaries of:

(i) the zone; and

(ii) any area within an offshore facility zone in which, because of paragraph 6.07J (2) (c), subregulation 6.07J (1) will not apply (a ***non-operational area***); and

[4] After regulation 6.05

insert

Division 6.1A Control of maritime security zones

Subdivision 6.1A.1 Preliminary

6.07A Purpose of Division 6.1A

(1) This Division provides for a scheme under which:

(a) a maritime security identification card (***MSIC***) is issued to identify a person who has been the subject of a background check; and

(b) a maritime industry participant will not allow a person to enter, or remain in, a maritime security zone unless he or she:

(i) displays a valid MSIC; or

(ii) is escorted by the holder of an MSIC.

(2) The Division includes requirements about:

(a) the display of MSICS; and

(b) issuing bodies for MSICs; and

(c) the issue of an MSIC to a person; and

(d) the expiry and cancellation of MSICs.

6.07B Definitions for Division 6.1A

In this Division:

AFP means the Australian Federal Police established under the *Australian Federal Police Act 1979*.

ASIO means the Australian Security Intelligence Organisation established under the *Australian Security Intelligence Organisation Act 1979*.

background check of a person means:

(a) a criminal records check of the person; and

(b) unless a security assessment of the person has previously been conducted — a security assessment of the person conducted by ASIO.

Commonwealth authority means:

(a) a Commonwealth department; or

(b) a body established for a public purpose by or under a law of the Commonwealth.

conviction (of a person for an offence) has the meaning given by subsection 85ZM (1) of the *Crimes Act 1914*, but does not include:

(a) a spent conviction (within the meaning given by subsection 85ZM (2) of that Act); or

(b) a conviction for an offence of which, under a law relating to pardons or quashed convictions, the person is taken never to have been convicted.

DIMIA means the Department administered by the Minister who administers the *Migration Act 1958*.

disqualifying offence means an offence mentioned in item 1 or 2 of Table 6.07C.

holder, of an MSIC, means the person to whom it is issued.

issuing body means a person or body authorised to issue MSICs.

MSIC means maritime security identification card.

security assessment has the same meaning as in Part IV of the *Australian Security Intelligence Organisation Act 1979*.

sentence includes a suspended sentence.

Note 1 Under the definition of ***conviction*** in subsection 85ZM (1) of the *Crimes Act 1914*, somebody is also taken to have been convicted of an offence if he or she has been convicted of the offence but no conviction has been recorded, and if a court has taken the offence into account in sentencing him or her for another offence: see paragraphs 85ZM (1) (b) and (c) of that Act.

Note 2 Under Part VIIC of the *Crimes Act 1914*, if somebody receives a free and absolute pardon for an offence against a law of the Commonwealth or a Territory because he or she was wrongly convicted of the offence, he or she is taken for all purposes never to have been convicted — see section 85ZR of that Act.

Note 3 Under the *Crimes Act 1914*, a person need not disclose convictions that:

(a) have been quashed (see section 85ZT); or

(b) are spent (see section 85ZV).

Note 4 Convictions for disqualifying offences do not become spent for the purposes of an authority assessing whether to issue the convicted person with an MSIC — see the *Crimes Act 1914*, paragraph 85ZZH (k), and the *Crimes Regulations 1990*, regulation 8 and Schedule 4.

6.07C Meaning of *maritime-security-relevant offence*

In this division, a ***maritime-security-relevant offence*** means an offence of a kind mentioned in an item in Table 6.07C or a similar offence against a law of a State or Territory, or of any other country or part of a country.

Table 6.07C Maritime-security-relevant offences

Item	Kind of offence
1	An offence mentioned in Chapter 5 of the *Criminal Code*. *Note* Offences for this item include treason, espionage and harming Australians
2	An offence involving the supply of weapons of mass destruction as mentioned in the *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995*
3	An offence mentioned in Part II of the *Crimes Act 1914*
4	An offence involving interference with aviation or maritime transport infrastructure including hijacking of an aircraft or ship, destruction of an aircraft or ship, carriage of dangerous goods on board an aircraft or ship, or endangering the security of aerodromes or ports
5	An 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 mentioned in Part 4 Division 73 of the Criminal Code

Item	Kind of offence
8	An offence involving the importing, exporting, supply or production of weapons, explosives or a trafficable quantity of drugs.

Note 1 Before 1 July 2006, a person who has been convicted of an offence mentioned in item 1 or 2 of Table 6.07C (a ***disqualifying offence***) must not enter a maritime security zone: see regulations 6.08D and 6.07K.

Note 2 On and after 1 July 2006, a person who has been convicted of a disqualifying offence must not be issued with an MSIC: see regulations 6.08C and 6.08H.

6.07D Meaning of *valid MSIC*

(1) For this Division, an MSIC is ***valid*** if:

(a) it is issued in accordance with Subdivision 6.1A.4; and

(b) it is not expired or cancelled; and

(c) it is not altered or defaced (permanently or temporarily); and

(d) the person who shows or displays it is the person to whom it was issued.

(2) However, an MSIC issued to a person who changes his or her name ceases to be valid 1 month after the day on which the change is made.

6.07E Meaning of *properly displaying*

(1) For this Division, somebody is ***properly displaying*** an MSIC only if it is attached to his or her outer clothing:

(a) above waist height; and

(b) at the front or side of his or her body; and

(c) with the whole front of the MSIC clearly visible.

(2) He or she is not ***properly displaying*** the MSIC if the photograph or anything else on it is obscured.

6.07F Meaning of *operational need*

For this Division, a person has ***an operational need*** to hold an MSIC if his or her occupation or business interests require, or

will require, him or her to have unmonitored access to a maritime security zone at least once each year.

Examples

1 a person whose work takes him or her into a zone;

2 a representative of a maritime industry participant that has a business connection with the zone;

3 a representative of an employee association whose members work in the zone;

4 a representative of an industry association whose members include a maritime industry participant that has a connection with the zone;

5 a representative of an issuing body.

6.07G Kinds of identification document

(1) This regulation sets out the criteria that a document must meet to qualify as a primary, secondary or tertiary identification document for somebody.

(2) A document is a ***primary identification document*** for somebody if it is:

(a) a certified copy (that is, a copy certified by a Registrar of Births or similar officer to be a correct copy) of the entry, in a register of births, of his or her birth; or

(b) a copy (certified under section 44 of the *Australian Citizenship Act 1948*) of a citizenship certificate granted to him or her; or

(c) a document issued to him or her under the law of another country that is evidence, under that law, that he or she is a citizen of that country; or

(d) a passport issued to him or her.

(3) A document is a ***secondary identification document*** for somebody if:

(a) it has on it a recent photograph of him or her, or his or her signature; and

(b) it is:

(i) a licence (for example, a driver's licence) issued to him or her under a law of the Commonwealth or a State or Territory; or

(ii) a government employee identification document issued to him or her; or

(iii) an Australian student identification document issued to him or her; or

(iv) a verifiable reference.

(4) In subregulation (3):

Australian student identification document means a card or document issued to a student at a tertiary education institution in Australia to identify him or her as a student at the institution.

government employee identification document means a document issued by or for the Commonwealth or a State or Territory to somebody employed by or for the Commonwealth or the State or Territory.

verifiable reference about somebody (the ***identified person***) means a reference from:

(a) a bank or similar financial institution; or

(b) somebody whose identity has been verified by means of:

(i) 2 primary identification documents; or

(ii) a primary identification document and a secondary identification document; or

(iii) a primary identification document and 2 tertiary identification documents; or

(c) a referee acceptable to the person or body that requires the identification of the identified person;

that:

(d) identifies the identified person by name; and

(e) certifies that the person who signed the reference has known the identified person by that name for at least 12 months; and

(f) is signed by or for the referee and by the identified person.

(5) A document is a ***tertiary identification document*** for somebody if:

(a) it sets out his or her name and address; and

(b) it is:

(i) a signed statement by his or her employer or former employer about that employment; or

(ii) a copy (certified by a Registrar of Titles or similar officer to be a correct copy) of a record issued under a law about land titles; or

(iii) a document issued by a rating authority from its records about land ownership or occupation; or

(iv) a document issued by a bank or similar financial institution from its records about a mortgage or other security that he or she gave to the bank or institution; or

(v) an extract from the electoral roll compiled by the Australian Electoral Commission; or

(vi) a record issued under a law in force in Australia other than a law about land titles.

6.07H Authentication of certain foreign documents

(1) In this regulation:

Hague Convention means the *Convention abolishing the Requirement of Legalisation for Foreign Public Documents*, done at the Hague on 5 October 1961.

(2) This regulation applies if a person presents to an issuing body, as an identification document, a document that is a public document for the purposes of the Hague Convention and was issued in a country (other than Australia) that is a Contracting State to that Convention.

(3) The body may require the person to have the authenticity of the document certified in accordance with that Convention.

Note The authentication procedure involves the endorsement on, or attachment to, the document of a certificate in a standard form. Details of the procedure and any fee payable should be available from the embassy of the country in which the document was issued.

Subdivision 6.1A.2 Display of MSICs

6.07I Definitions for Subdivision 6.1A.2

In this Subdivision:

escort means a person who escorts, or continuously monitors, another person in a maritime security zone.

Note Unless exempt, an escort must hold a valid MSIC: see regulation 6.07J.

visitor, to a maritime security zone, means a person who is entitled to be in the zone because he or she is being escorted or continuously monitored.

6.07J Requirement to display MSIC in maritime security zones

(1) A person commits an offence if:

(a) he or she is in a maritime security zone; and

(b) he or she fails to properly display a valid MSIC.

Penalty:

(c) for a first offence — 5 penalty units; or

(d) for a second offence within 2 years of an offence — 10 penalty units; or

(e) for a third or subsequent offence within 2 years of an offence — 20 penalty units.

(2) Subregulation (1) does not apply to:

(a) a visitor to the zone, if his or her escort:

(i) is displaying a valid MSIC; or

(ii) is carrying a valid MSIC but, under regulation 6.07M, is exempt from the requirement to display it;

(iii) is exempt, under regulation 6.07M, from the requirement to carry a valid MSIC; or

(b) the holder of an identification document issued by an arm of the Defence Force who:

(i) is displaying his or her identification document; and

(ii) is in the zone as part of his or her duties for the Force; or

(c) a person who is in a non-operational area (within the meaning given in subparagraph 5A.85 (1) (a) (ii)) of an offshore facility zone.

(3) A contravention of subregulation (1) is an offence of strict liability.

(4) Subregulation (1) does not apply before 1 July 2006.

6.07K Person given disqualifying offence not to enter maritime security zone

(1) A person who has been given a disqualifying notice by the Secretary under regulation 6.08D must not enter a maritime security zone.

Penalty: 5 penalty units.

(2) Subregulation (1) does not apply to a person who is a visitor to a zone for the purpose of boarding or leaving a vessel as part of a recreational activity.

(3) A contravention of subregulation (1) is an offence of strict liability.

6.07L Offence — failure to properly escort visitor

(1) An escort is guilty of an offence if he or she fails to escort, or continuously monitor, a visitor in accordance with the procedures set out in the maritime security plan of the maritime industry participant concerned.

Penalty: 5 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.

6.07M Persons exempted by Secretary from requirement to hold, carry or display MSIC

(1) Despite regulation 6.07J, somebody to whom the Secretary has given an exemption under this regulation need not display an MSIC in a maritime security zone.

(2) Within 30 days after receiving an application, the Secretary must:

(a) give or refuse the exemption; and

(b) notify the person in writing of the decision and, if the decision is a refusal, the reasons for it.

(3) On the Secretary's own initiative, or on written application by a person, the Secretary may give a person, or all persons in a specified class, exemption from the requirement, in 1 or more specified maritime security zones, to:

(a) hold an MSIC; or

(b) carry an MSIC; or

(c) display an MSIC.

(4) Before giving or refusing an exemption, the Secretary must consider:

(a) why the exemption is necessary; and

(b) the likely effect of the proposed exemption on maritime transport security in the zone; and

(c) how long the proposed exemption will last, if it is given; and

(d) anything else relevant that the Secretary knows about.

(5) The Secretary may give an exemption:

(a) for a particular period and subject to a condition or conditions mentioned in the exemption; or

(b) limited to a particular zone or part of a zone.

(6) If the Secretary gives an exemption to all persons in a specified class, the Secretary must publish a notice of the exemption in the *Gazette*.

6.07N Access by emergency personnel

(1) Nothing in this Division requires or authorises a maritime industry participant to prevent any of the following having access to any part of a maritime security zone:

(a) members of the Defence Force who are responding to an event or threat of unlawful interference with maritime transport in the zone;

(b) ambulance, rescue or fire service officers who are responding to an emergency.

(2) A requirement of this Part to display an MSIC does not apply to a person referred to in paragraph (1) (a), (b) or (c).

Subdivision 6.A1.3 MSIC issuing bodies

6.07O Application for authorisation to issue MSICs

(1) The following may apply, in writing, to the Secretary for authorisation as an issuing body:

(a) a maritime industry participant;

(b) a body representing participants;

(c) a body representing employees of participants;

(d) a Commonwealth authority.

Note Knowingly making a false or misleading statement in an application is an offence punishable by imprisonment for 12 months — see the *Criminal Code*, section 136.1.

(2) However, a participant may engage an agent to issue MSICs and the agent may apply to be an issuing body.

(3) An application must be accompanied by a statement setting out the applicant's proposed MSIC plan.

(4) An applicant is entitled to perform the functions or exercise the powers of an issuing body only if the applicant's MSIC plan is approved by the Secretary.

6.07P Decision on application

(1) If the Secretary needs more information to deal with an application under regulation 6.07O, the Secretary may ask the applicant, in writing, to provide the information.

(2) Before the end of 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (1), before the end of 30 days after receiving the information), the Secretary must:

(a) authorise, or refuse to authorise, the applicant as an issuing body; and

(b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(3) If the Secretary has not authorised, or refused to authorise the applicant as an issuing body within the period allowed by subregulation (2), the Secretary is taken to have refused to authorise the applicant as an issuing body.

(4) The Secretary must not authorise the applicant as an issuing body unless the Secretary is satisfied that:

(a) the applicant's MSIC plan is apparently adequate to give effect to the proposed plan's purposes; and

(b) authorising the applicant as an issuing body would not be likely to be a threat to maritime transport security.

(5) The Secretary may authorise an applicant as an issuing body subject to a condition set out in the instrument of authorisation.

6.07Q What an MSIC plan is

(1) An ***MSIC plan*** sets out procedures to be followed for the following purposes:

(a) the issue and production of MSICs;

(b) the design, distribution and storage of sample MSICs for training purposes, if the issuing body proposes to issue such MSICs;

(c) the safekeeping, secure transport and disposal of MSICs and associated equipment;

(d) the recovery and secure destruction of issued MSICs that are no longer required;

(d) the security of records in relation to applicants for MSICs;

(f) lost, destroyed or stolen MSICs;

(g) ensuring that MSICs are returned to issuing bodies when they are no longer required.

(2) An MSIC plan must also set out the procedures that will be followed if the applicant is authorised as an issuing body and the authorisation is later revoked, including procedures to ensure that information about applications for MSICs, and holders of MSICs, is appropriately preserved.

Note An applicant for authorisation as an issuing body must provide with its application a statement of its proposed MSIC plan— see regulation 6.07O.

6.07R Issuing body to give effect to MSIC plan

(1) An issuing body must not fail to give effect to its MSIC plan.

Penalty: 50 penalty units.

(2) Without limiting subregulation (1), an issuing body fails to give effect to its MSIC plan if it:

(a) fails to do something that its MSIC plan requires that it do; or

(b) does something that its MSIC plan requires that it not do; or

(c) does something that its MSIC plan requires that it do, but does so in a way that contravenes the plan.

(3) A contravention of subregulation (1) is an offence of strict liability.

(4) However, an issuing body may apply, in writing, to the Secretary for exemption from giving effect to its MSIC plan in a particular case or respect.

(5) If the Secretary needs more information to deal with an application, the Secretary may ask the applicant, in writing, to provide the information.

(6) Within 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (5), within 30 days after receiving the information), the Secretary must:

(a) grant or refuse the exemption; and

(b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(7) If the Secretary has not approved, or refused to approve, the exemption within the period allowed by subregulation (6), the Secretary is taken to have refused to approve the exemption.

(8) The Secretary may also grant, on his or her own initiative, an issuing body a written exemption from giving effect to its MSIC plan in a particular case or respect.

(9) Before granting or refusing an exemption under this regulation, the Secretary must consider:

(a) the justification for the proposed exemption; and

(b) the likely effect of the proposed exemption on each of the plan purposes; and

(c) how long the proposed exemption will be for, if it is granted; and

(d) anything else relevant that the Secretary knows about.

(10) The Secretary may grant an exemption for a particular period and subject to a condition mentioned in the exemption.

6.07S Direction to vary MSIC plan

(1) If an issuing body's MSIC plan is not adequate to give effect, in all circumstances, to any 1 or more of the plan purposes, the Secretary may direct the body, in writing, to vary the plan.

(2) The Secretary must not give such a direction in relation to a plan purpose unless the Secretary is satisfied that the variation is appropriate to make the plan adequate for that purpose.

(3) A direction must:

(a) indicate the variation needed; and

(b) state the time within which the issuing body must submit an appropriately varied plan to the Secretary.

(4) An issuing body must comply with such a direction.

Note Regulation 6.07V provides for the revocation of the authorisation of a body that does not comply with a direction.

6.07T Variation of MSIC plan by issuing body

(1) An issuing body may:

(a) review its MSIC plan at any time; and

(b) submit a written proposed variation of the plan to the Secretary for approval.

(2) If the Secretary needs more information to deal with an application, the Secretary may ask the applicant, in writing, to provide the information.

(3) Before the end of 30 days after receiving the proposed variation (or, if the Secretary asks for more information under subregulation (2)), before the end of 30 days after receiving the information), the Secretary must:

(a) approve or refuse to approve the variation; and

(b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(4) If the Secretary has not approved, or refused to approve, the plan within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the plan.

(5) The Secretary must approve the variation if the plan, as varied, will give effect to the plan purposes.

6.07U Issuing bodies' staff

(1) An issuing body other than a Commonwealth authority must not allow a person to be directly involved in the issue of MSICs unless he or she is able to satisfy the security-relevant criteria for the issue of an MSIC.

Penalty: 20 penalty units.

(2) A Commonwealth authority that is an issuing body must not allow a person to be directly involved in the issue of MSICs unless he or she is able to satisfy the security-relevant criteria for the issue of an MSIC.

(3) Despite subregulations (1) and (2) the Secretary may approve the involvement of a person in the issue of MSICs if:

(a) a security assessment of the person is qualified; but

(b) the Secretary is satisfied that the involvement of the person in the issue of MSICs would not constitute a threat to maritime transport security.

(4) For subregulations (1) and (2), a person ***satisfies the security-relevant criteria*** for the issue of an MSIC if he or she is able to satisfy the criteria for the issue of an MSIC set out in paragraphs 6.08C (1) (b), (c), (d) and (e).

6.07V Revocation of authorisation for cause

(1) The Secretary must revoke an issuing body's authorisation as an issuing body if in the opinion of the Secretary:

(a) the body's MSIC plan is apparently no longer adequate to give effect to a plan purpose and it is unlikely that a direction under regulation 6.07S will make the plan adequate for that purpose; or

(b) allowing the body's authorisation to continue would be likely to be a significant threat to maritime transport security; or

(c) the body does not comply with a direction of the Secretary under regulation 6.07S.

(3) The Secretary may revoke the authorisation of an issuing body if the body contravenes:

(a) a condition of its authorisation; or

(b) its MSIC plan.

(4) For subregulation (3), the Secretary must consider:

(a) the kind and seriousness of the contravention; and

(b) whether the issuing body has previously contravened a condition of its authorisation or its MSIC plan.

(5) As soon as practicable after revoking the authorisation of a body under this regulation, the Secretary must notify the body in writing of the revocation and the reasons for the revocation.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(6) The revocation takes effect when written notice of the revocation is given to the body.

6.07W Revocation of authorisation at request of issuing body

(1) The Secretary must revoke the authorisation of a body as an issuing body if the body asks the Secretary, in writing, to do so.

(2) A revocation under subregulation (1) takes effect when the request was made.

6.07X Re-applying for authorisation

A body whose authorisation is revoked may apply under regulation 6.07O for a new authorisation.

6.07Y What happens if issuing body no longer able to issue MSICs

(1) This regulation applies if:

(a) the authorisation of an issuing body (the ***original issuing body***) is revoked; or

(b) the body ceases to exist; or

(c) for any other reason, the body no longer performs the functions or exercises the powers of an issuing body.

(2) The Secretary may authorise, in writing, another person to perform the functions, and exercise the powers, of the original issuing body (other than functions and powers relating to the documents mentioned in paragraph (5) (a)) in relation to MSICs issued by that body.

(3) An MSIC issued by the original issuing body that is in force at the time of such an authorisation is not affected by:

(a) the body having ceased to exist; or

(b) the new authorisation.

(4) The person authorised under subregulation (2) is taken to be the issuing body for the MSIC, but is not responsible for the actions of the original issuing body in relation to the MSIC before the authorisation.

(5) An authorisation:

(a) is subject to the condition that any documents used to decide about the eligibility of a person for an MSIC are to be held by the Secretary; and

(b) may be subject to another condition specified in it.

Subdivision 6.1A.4 MSICs: issue, expiry and cancellation

6.08A Meaning of *adverse criminal record*

For this Subdivision, a person has an ***adverse criminal record*** if he or she has been convicted of a maritime-security-relevant offence and sentenced to imprisonment (including periodic detention, home-based detention, and detention until the rising of the court, but not including a sentence of community service).

Note For the meaning of ***maritime-security-relevant offence***, see regulation 6.07C.

6.08B MSICs — application for issue

(1) A person may, in writing, apply to an issuing body for the issue of an MSIC if he or she has an operational need to hold an MSIC.

(2) An applicant who has turned 18 must prepare a signed form of consent to background checking of the applicant and:

(a) if applying before 1 July 2006 — send the form to the AFP; or

(b) if applying on or after 1 July 2006 — include the form with the application.

6.08C MSICs — issue

(1) An issuing body may issue an MSIC to a person only if:

(a) the person has an operational need to hold an MSIC; and

(b) the person has verified his or her identity by showing the issuing body:

(i) a primary identification document; and

(ii) either:

(A) a secondary identification document; or

(B) 2 tertiary identification documents; and

(c) either:

(i) has shown the issuing body a document that is evidence that the person is an Australian citizen (for example, his or her Australian birth certificate, Australian passport or Australian naturalisation certificate); or

(ii) the issuing body is satisfied that he or she holds a visa entitling him or her to work in Australia; and

(d) the issuing body has been notified in writing that a security assessment of the person has been made, and:

(i) the assessment was not adverse; or

(ii) if the assessment was qualified — the issuing body has not been directed by the Secretary under subregulation 6.08H (2) not to issue an MSIC to the person.

(e) the issuing body has been notified in writing that a criminal records check of the person has been made, and:

(i) the check shows that the person does not have an adverse criminal record; or

(ii) if the check shows that the person has an adverse criminal record — the Secretary has approved an

application to issue an MSIC to the person under paragraph 6.08F (3) (a).

Penalty: 50 penalty units.

(2) For subparagraphs (1) (e) (i) and (ii):

(a) from 1 October 2005 to the end of 30 June 2006 — the Secretary; or

(b) on and after 1 July 2006 — the issuing body;

must decide whether the criminal records check shows that the person has an adverse criminal record.

(3) An offence against subregulation (1) is an offence of strict liability.

(4) In the case of a person who is under 18, the issuing body may issue an MSIC to him or her despite paragraphs (1) (d) and (e) if he or she meets the criteria in paragraphs (1) (a), (b) and (c).

Note An MSIC issued under subregulation (3) ceases to be valid 6 months after the holder turns 18: see paragraph 6.08I (2) (a).

(5) If a person's MSIC is cancelled at his or her request under regulation 6.08N and, less than 12 months after the cancellation, the person:

(a) has an operational need to hold an MSIC; and

(b) gives an issuing authority a statutory declaration stating that, since the cancellation, no relevant circumstance of the person has changed;

the issuing body may issue the MSIC to him or her despite anything in subregulation (1).

(6) An issuing body may issue an MSIC subject to a condition, but must notify the holder in writing what the condition is.

Example

A condition that background checking of the holder is carried out more frequently than required by these Regulations.

(7) An issuing body may issue MSICs only in accordance with its MSIC plan.

6.08D Issue of disqualifying offence notice

(1) This regulation applies if, before 1 July 2006, the background check of an applicant for an MSIC reveals that:

(a) he or she has been convicted of a disqualifying offence; or

(b) the security assessment of the person is adverse and is not a qualified security assessment.

(2) The Secretary must send the person a notice in writing (a ***disqualifying notice***) that informs the person about the results of the background check and the effect of regulation 6.07K in relation to the person.

6.08E Issue of MSICs to ASIC holders

An issuing body may issue an MSIC to a person without verifying that the person has satisfied the criteria set out in subregulation 6.08C (1) if the person:

(a) holds an ASIC issued under the *Aviation Transport Security Regulations 2005*; and

(b) has an operational need for an MSIC.

Note The MSIC expires on the same day as the ASIC: see paragraph 6.08I (2) (c).

6.08F MSICs — Secretary's approval of issue in certain cases

(1) If:

(a) a person is not eligible to be issued an MSIC only because he or she has an adverse criminal record; and

(b) he or she has not been convicted of a disqualifying offence;

an issuing body or the applicant may apply to the Secretary, in writing, for approval to issue an MSIC to the person.

(2) If the Secretary needs more information to deal with an application, the Secretary may ask the issuing body or applicant, in writing, to provide the information.

(3) Within 30 days after receiving an application (or, if the Secretary has asked for information under subregulation (2), after receiving the information), the Secretary must:

(a) approve, or refuse to approve, in writing, the issuing of the MSIC; and

(b) notify the body, or applicant, in writing of the decision and, if the decision is a refusal, notify the applicant of the reasons for the decision.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(4) If the Secretary has not approved, or refused to approve, the issue of the MSIC within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the issue of the MSIC.

(5) Before approving or refusing to approve the issue of the MSIC to a person who is not eligible to be issued an MSIC only because, under paragraph 6.08C (1) (e), the person's criminal record prevents him or her being issued with an MSIC, the Secretary must decide whether the person constitutes a threat to maritime transport security by considering:

(a) the nature of the offence the person was convicted of; and

(b) the length of the term of imprisonment imposed on him or her; and

(c) if he or she has served the term, or part of the term — how long it is, and his or her conduct and employment history, since he or she did so; and

(d) 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

(e) anything else relevant that the Secretary knows about.

(6) The Secretary may give an approval subject to a condition, but must notify the issuing body in writing what the condition is.

Example

A condition that background checking is conducted at specified intervals.

6.08G Report to Secretary of refusal to issue MSICs in certain cases

(1) If, on or after 1 July 2006, an issuing body refuses to issue an MSIC to an applicant because the applicant fails to satisfy a criterion in paragraph 6.08C (1) (c) or (e), the issuing body must, within 7 days of the decision, give the Secretary a written report that sets out:

(a) the applicant's name, address and date of birth; and

(b) the reasons for the refusal.

(2) The Secretary may pass the information mentioned in paragraph (1) (a) on to other issuing bodies if he or she thinks that doing so will help to prevent unlawful interference with maritime transport.

6.08H Persons the subject of adverse or qualified security assessments

(1) If a security assessment of a person is an adverse security assessment, the Secretary must direct an issuing body that proposes to issue an MSIC to the person that the MSIC is not to be issued.

(2) The Secretary may direct an issuing body not to issue an MSIC to a person if, on the basis of a security assessment of the person that is a qualified security assessment, the Secretary is satisfied that the holding of an MSIC by the person would constitute a threat to maritime transport security.

(3) A direction under subregulation (1) or (2) must be in writing.

(4) An issuing body must not issue an MSIC to a person in contravention of a direction under subregulation (1) or (2).

Penalty: 20 penalty units.

Note If an adverse or qualified security assessment about a person is provided to a Commonwealth authority, the authority must notify the person in writing within 14 days (including a copy of the assessment) and must notify him or her how to apply to the Administrative Appeals Tribunal for review of the assessment — see the *Australian Security Intelligence Organisation Act 1979*, section 38.

6.08I MSICs — period of issue and expiry

(1) Unless earlier cancelled, an MSIC expires 5 years after the day when the relevant criminal records check conducted by the AFP is completed.

(2) However:

(a) an MSIC issued to a person under 18 in reliance on subregulation 6.08C (3) must expire no later than 6 months after the person's 18th birthday; and

(b) an MSIC issued to a person who is entitled to remain in Australia because he or she holds a visa must expire no later than the day on which the person's visa expires; and

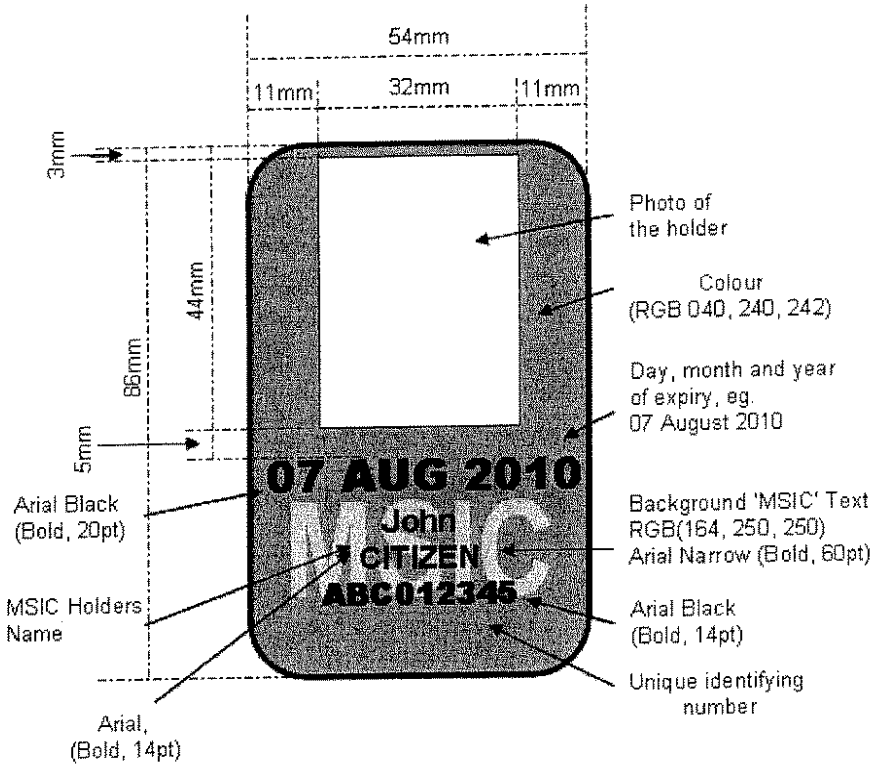
(c) an MSIC issued under regulation 6.08E must expire on the same day as the ASIC mentioned in paragraph 6.08E (a).

6.08J Form of MSICs other than temporary MSICs

(1) This regulation does not apply to a temporary MSIC.

Note For details about temporary MSICs, see regulation 6.08K.

(2) The form of an MSIC is as follows:



(3) An MSIC must comply with the following requirements:

(a) the dimensions of the MSIC, and of each of its parts, must be as shown in the diagram in subregulation (2);

(b) where the diagram indicates a particular colour, type-face or type size, that colour, type-face or type size must be used;

(c) the photograph of the holder must be a recent (that is, taken within 6 months before the issue of the MSIC) photograph of the holder, showing the holder's full face and his or her head and shoulders;

(d) the photograph must be protected against tampering by a method that is approved by the Secretary and identified in a notice published in the *Gazette*; or

(e) the first name and surname must be those that the holder normally uses;

(f) the number must be unique among MSICs issued by that issuing body and include the issuing body identifier as directed by, or agreed with, the Secretary;

(g) if the issuing body is the Australian Customs Service, the word 'Customs' must appear on the MSIC;

(h) the expiry date must be expressed as *day abbreviated month year*, where ***abbreviated month*** means the first 3 letters of the name of the month of expiry.

(4) An MSIC that is issued to a law enforcement officer or an officer or employee of ASIO may bear the holder's name on the back of the MSIC.

(5) The Secretary may approve the issue of an MSIC showing the holder's name on the back if the Secretary is satisfied that having the holder's name on the front would put the holder's personal security at risk.

(6) An issuing body must not issue an MSIC that does not comply with subregulations (2), (3), (4) and (5).

Penalty: 50 penalty units.

(7) An offence under subregulation (6) is an offence of strict liability.

Note For ***strict liability***, see section 6.1 of the *Criminal Code*.

6.08K Temporary MSICs

(1) A temporary MSIC may be issued to a person by:

(a) an issuing body; or

(b) if it acts in accordance with its maritime security plan — a maritime industry participant;

if:

(c) the person is the holder of another MSIC and has forgotten the other MSIC, or it has been lost, stolen or destroyed; and

(d) the issuing body or participant is satisfied about the identity of the person.

(2) The issuing body or participant may issue an MSIC that is valid only for a specified period.

6.08L Issue of replacement MSICs

(1) An issuing body may issue a replacement MSIC to the holder of another MSIC if he or she has lost the other MSIC, or it has been stolen or destroyed, and:

(a) he or she has made a statutory declaration setting out the circumstances of the loss, theft or destruction; or

(b) if the other MSIC has been stolen — he or she has given the issuing body a copy of a police report, or other information issued by the police, regarding the theft.

(2) If the holder of an MSIC changes his or her name, an issuing body may issue a replacement MSIC to the holder after:

(a) the holder provides written evidence of the change; and

(b) the issuing body notifies ASIO of the change of name and ASIO acknowledges receipt of the notification.

(3) A replacement MSIC must expire no later than the earlier MSIC would have expired.

6.08M Cancellation of MSICs

(1) An issuing body must immediately cancel an MSIC issued by the body if:

(a) the body finds out that the MSIC was not issued in accordance with the body's MSIC plan; or

(b) the Secretary finds out that the MSIC was not issued in accordance with the body's MSIC plan and notifies the issuing body in writing; or

(c) the Secretary has notified the issuing body in writing that a security assessment of the holder was adverse; or

(d) the body finds out that the holder is or has become an unlawful non-citizen; or

(e) the body finds out that the holder has been convicted of a disqualifying offence; or

(f) the holder no longer has an operational need to hold an MSIC; or

(g) the body finds out that, for a continuous period of 12 months, the holder has not had an operational need to hold an MSIC.

Note for paragraph (1) (e) See regulation 6.07B for the meaning of ***disqualifying offence***.

(2) As soon as practicable after an issuing body cancels an MSIC under subregulation (1), the body must notify the holder, in writing, that the MSIC has been cancelled and the reasons for the cancellation.

Note Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the notice reviewed.

(3) A cancellation under subregulation (1) takes effect when the holder is notified of it in writing.

6.08N Cancellation of MSICs at holder's request

(1) An issuing body must cancel an MSIC issued by the body if the holder of the MSIC asks the body to cancel it.

(2) A cancellation under subregulation (1) takes effect when the MSIC is returned to the issuing body.

6.08O Report to Secretary of cancellation of MSICs in certain cases

(1) If an issuing body cancels an MSIC on the basis of paragraph 6.08M (1) (c), (d), or (e), the issuing body must, within 7 days of the decision, give the Secretary a written report that sets out:

(a) the holder's name, address and date of birth; and

(b) the reasons for the cancellation.

(2) The Secretary may pass the information mentioned in paragraph (1) (a) on to other issuing bodies if he or she thinks that doing so will help to prevent unlawful interference with maritime transport.

6.08P Return of MSICs that have expired etc

(1) The holder of an MSIC must return it to an issuing body 30 days or less after:

(a) the MSIC expires; or

(b) the holder is notified that it has been cancelled; or

(c) the MSIC has been damaged, altered or defaced (permanently or temporarily).

Penalty: 10 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.

6.08Q Holder no longer needing MSIC

(1) The holder of an MSIC is guilty of an offence if:

(a) he or she becomes aware of circumstances that will result in him or her not having an operational need to hold the MSIC for 12 months; and

(b) he or she fails to return it to an issuing body within 30 days of becoming aware of the circumstances.

Penalty: 5 penalty units.

(2) Strict liability applies to paragraph (1) (b).

6.08R Notification of lost etc MSICs

(1) The holder of an MSIC commits an offence if:

(a) the MSIC has been lost, stolen or destroyed; and

(b) the holder of the MSIC knows about the loss, theft or destruction; and

(c) he or she does not:

(i) make a report, in the form of a statutory declaration, of the loss to the issuing body that issued the MSIC within 7 days of becoming aware of the loss, theft or destruction; or

(ii) if the MSIC was stolen — give the issuing body a copy of a police report, or other information issued

by the police, regarding the theft, within 7 days of becoming aware of the theft.

Penalty: 10 penalty units.

(2) Strict liability applies to paragraph (1) (c).

(3) However, subregulation (1) does not apply if the MSIC has been destroyed by the issuing body that issued it.

Subdivision 6.1A.5 Powers of security officers in relation to MSICs

6.08S Directions to show valid MSICs or other identification

(1) In this regulation:

exempt person, in relation to a part of a maritime security zone, means somebody who, under the Act or these Regulations, is not required to properly display a valid MSIC in that part of that zone.

security officer means:

(a) a law enforcement officer; or

(c) a maritime security inspector.

(2) If:

(a) a security officer knows, or has reason to believe, that a person who is in a part of a maritime security zone is an exempt person; and

(b) the person is apparently not properly displaying a valid MSIC;

the security officer may direct the person to show him or her a valid MSIC or identification that establishes that he or she is an exempt person.

(3) Before directing the person to do so, the security officer must show the person:

(a) the officer's identity card; or

(b) another appropriate form of identification.

(4) A person must comply with a direction of a security officer under subregulation (2).

Penalty: 10 penalty units.

Subdivision 6.1A.6 Record-keeping

6.08T Register of MSICs

(1) An issuing body must keep a register in accordance with this regulation.

(2) The register must contain the following details of each MSIC issued by the body to a person:

(a) his or her name and telephone number (if any);

(b) a copy of the photograph that appears on his or her MSIC;

(c) subject to subregulation (3), his or her residential address;

(d) the general reason that he or she has an operational need to hold an MSIC;

(e) the documents used to decide about his or her eligibility for an MSIC;

(f) the date of the beginning of the current period during which he or she has continuously held an MSIC;

(g) the unique number of the MSIC;

(h) its date of issue;

(i) its date of expiry;

(j) if applicable, the date on which it was cancelled;

(k) if applicable, the date or dates on which it was reported lost, stolen or destroyed.

(3) The register need not contain the residential address of an MSIC holder who is:

(a) a law enforcement officer; or

(b) an officer or employee of ASIO; or

(c) an employee of a Commonwealth authority.

6.08U Other records

(1) An issuing body must maintain records that are sufficient to demonstrate that it has complied with its MSIC plan.

(2) The body must retain the record of issue of an MSIC to a person for at least 7 years after the creation of the record.

(3) The records may be kept by means of a computer or in any other form that can be conveniently audited.

(4) The issuing body must hold the records at its office.

(5) The issuing body must allow a maritime security inspector to inspect the records on request subject to reasonable notice.

6.08V Annual reporting

An issuing body must report to the Secretary in writing, within 1 month after the end of each financial year:

(a) the total number of MSICs issued by the body; and

(b) the number of MSICs issued by the body that have not expired and have not been cancelled; and

(c) the number of MSICs issued by the body that have expired or been cancelled but have not been returned to the body; and

(d) the number of MSICs issued by the body that were cancelled in the financial year to which the report relates;

(e) the number of MSICs issued by the body that expired in that financial year.

Penalty: 20 penalty units.

Subdivision 6.1A.7 Review of decisions

6.08W Definitions

In this Subdivision:

AAT Act means the *Administrative Appeals Tribunal Act 1975*.

decision has the same meaning as in the AAT Act.

Tribunal means the Administrative Appeals Tribunal.

6.08X Reconsideration of decisions in relation to MSICs and related matters

Decisions in relation to issuing bodies

(1) Application may be made to the Secretary for review of a decision of the Secretary:

(a) to refuse to authorise a person as an issuing body; or

(b) to impose a condition on an issuing body; or

(c) to direct an issuing body to vary its MSIC plan; or

(d) to refuse to approve a variation of an issuing body's MSIC plan; or

(e) to refuse to exempt an issuing body from giving effect to its MSIC plan in a particular case or respect; or

(f) to impose a condition on an exemption; or

(g) to revoke an issuing body's authorisation.

Decisions in relation to adverse maritime security status

(2) Application may be made to the Secretary for review of a decision of the Secretary that on the basis of a qualified security assessment, a person has an adverse maritime security status.

Decisions in relation to issue and cancellation of MSICs

(3) Application may be made to the Secretary for review of a decision of:

(a) the Secretary to:

(i) refuse to authorise the issue of an MSIC; or

(ii) impose a condition on an MSIC; or

(b) an issuing body to:

(i) refuse to issue an MSIC to somebody; or

(ii) issue an MSIC subject to a condition; or

(iii) cancel an MSIC.

Decisions in relation to wearing and use of MSICs

(4) Application may be made to the Secretary for review of a decision of the Secretary:

(a) to refuse to exempt somebody from displaying a valid MSIC in a maritime security zone, or part of such an area; or

(b) to impose a condition on such an exemption.

Decisions in relation to the substituted exercise of the powers of an issuing body

(5) Application may be made to the Secretary for review of a decision of the Secretary:

(a) to authorise, or refuse to authorise, a person to perform the functions, or exercise the powers, of an issuing body; or

(b) to authorise a person to perform the functions or exercise the powers of an issuing body subject to a condition.

Decisions in relation to issue of disqualifying notice

(6) Application may be made to the Secretary for review of a decision of the Secretary to issue a disqualifying notice under regulation 6.07K.

6.08Y If Secretary makes no decision

If person applies to the Secretary under regulation 6.08X for review of a decision and, 30 days after making the application, the Secretary has not notified his or her decision about the application to the applicant, the Secretary is taken to have refused to vary the original decision.

6.08Z AAT review of Secretary's decisions

Application may be made under the AAT Act to the Tribunal for review of a decision made by the Secretary as a result of an application under regulation 6.08W.

Subdivision 6.1A.8 Miscellaneous

6.09A Cost recovery

An issuing body may recover the reasonable costs of the issue of an MSIC from the person who asks the body to issue the MSIC.

Note

1. All legislative instruments and compilations are registered on the Federal Register of Legislative Instruments kept under the *Legislative Instruments Act 2003*. See www.frli.gov.au.