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