Chapter 5

The Aviation and Maritime Security Identification Card system

Introduction

5.1 The Aviation Security Identification Card (ASIC) and Maritime Security Aviation Card (MSIC) schemes were introduced to protect the aviation and maritime workforces from infiltration by terrorist organisations and individuals who may help to facilitate an act of terror.

5.2 Specifically, the security card systems were introduced through aviation and maritime national security legislation to help safeguard Australia's aviation and maritime transport systems and offshore facilities from terrorism and unlawful interference.[1] However, the schemes were not designed to specifically target criminality and organised crime.

5.3 The second chapter of this report discusses the relevant legislation, namely the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Act 2003* (MTOFSA). The committee has expressed its concern that the legislation focuses narrowly on counterterrorism considerations, and argued for an extension of the legislation's focus to include serious and organised crime. The committee considers that the ASIC and MSIC schemes enacted under that legislation should also be extended to protect aviation and maritime workforces from infiltration by organised criminal networks. This chapter addresses that issue and others raised during the course of the inquiry.

The ASIC and MSIC schemes

5.4 The ASIC and MSIC schemes are established in the Aviation Transport Security Regulations 2005 (Aviation Regulations) and Maritime Transport and Offshore Facilities Regulation 2003 (Maritime Regulations), and are administered by the Department of Infrastructure and Transport.

5.5 The schemes require all persons needing unescorted access to aviation or maritime security zones to display an ASIC or MSIC. The cards themselves are not necessarily access cards and they do not provide the right of entry to a facility within an aviation or maritime security zone. Rather, they represent that an individual has passed certain background checks. However, the committee is aware that some issuing bodies (such as airports, airlines or stevedore companies) integrate the ASIC or MSIC and their own private access cards into a single card for convenience.

---

1 See Chapter 2 for a description of the aims of the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003*.

5.6 Workers who may require an ASIC or MSIC include most employees based at airports, port and offshore oil and gas facilities as well as maintenance and transport workers servicing these facilities. As at 30 June 2010, there were almost 130 000 validly issued ASICs and almost 140 000 valid issued MSICs recorded on the AusCheck database.[2]

5.7 In order to obtain an ASIC or MSIC, a person with an operational need to access an aviation or maritime security zone must apply in writing through an Issuing Body, which is an industry association or private company that has been authorised by the Department of Infrastructure to issue ASICs or MSICs.[3] As part of the application process, individuals must provide the following information:

- proof of identity documents;
- confirmation of the right to work in Australia; and
- evidence of operational need to have an ASIC or MSIC.[4]

5.8 All individuals who apply for an ASIC or MSIC must be background checked to determine eligibility. The background checking is conducted by AusCheck on behalf of the issuing body. AusCheck coordinates the following three vetting arrangements that underpin both the ASIC and MSIC schemes:

- a criminal record check by CrimTrac, used to determine if an applicant has an adverse criminal record;
- a security assessment by ASIO; and
- if required, a right to work check by the Department of Immigration and Citizenship (DIAC).[5]

5.9 Should an individual's criminal record check be found to be adverse, they may not be issued with a card. However, an adverse finding generally requires that the applicant have been *imprisoned* as consequence of a conviction for a prescribed offence, with some caveats.[6] Several witnesses providing evidence to the committee were concerned that workers convicted of certain offences, but not imprisoned, were still eligible for the card, an issue which is addressed below.

---

2 Australian National Audit Office, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 13.

3 Attorney-General's Department, *Submission 14*, p. 5.

4 AGD, *Submission 14*, p. 5.

5 Ms Tamsyn Harvey, AusCheck, *Committee Hansard*, 17 February 2011, p. 21.

6 Changes in 2010 to the MSIC scheme mean that convictions for terrorism-related offences that did not result in imprisonment may in fact disqualify an applicant. Additionally, an ASIC may be denied if the applicant has been convicted of a relevant offence in the last 12 months and it is their second relevant conviction, even if neither resulted in imprisonment.

5.10 The criminal record and security assessments for both the ASIC and MSIC do not apply to people under the age of 18. Cards issued under this clause cease to be valid six months after the holder turns 18.

Features of the ASIC scheme

5.11 ASIC cards are issued for a period of two years, after which they must be renewed, including a fresh background check. There are two broad categories of ASIC card: red cards allow access to secure areas including the airside security zone, while grey cards allow access to secure areas, but not including the airside security zone.

5.12 Both red and grey ASICs can be issued as permanent (2 year) or temporary passes. The regulations specify that a temporary pass may be issued to the holder of a permanent ASIC in the event that the permanent pass has been left at home, damaged or stolen. Overseas workers with similar passes from that jurisdiction may receive a temporary pass while working for short stints in Australia.

5.13 ASIC card holders are obliged to notify issuing bodies of certain matters. They must return their ASIC to the issuing body within one month after it expires, is cancelled, has been damaged, altered or defaced; or they no longer have an operational need to enter a secure area.

5.14 In addition, card holders must notify their issuing body: within seven days, if their ASIC is lost, stolen or destroyed; within 30 days, if they change their name; and within seven days, if they are convicted of an aviation-security relevant offence. Notification must usually be in the form of a statutory declaration or police report. In 2010, the penalty for not doing so was raised from $2200 to $5500.[7]

Visitor Identification Card

5.15 Visitor Identification Cards (VICs) can be issued to individuals who need to enter secure aviation areas but do not have a valid ASIC. They must be supervised at all times by a holder of an ASIC.[8] VICs are generally only valid for up to one month, unless the issuing body has special approval to issue cards for longer duration, with the maximum possible being three months.

5.16 An issuing body must not knowingly issue a VIC to somebody who has been refused an ASIC.

---

7 AGD, answer to question on notice, 17 February 2011 (received 18 March 2011).

8 If they are working in an area in a secure zone with no access to aircraft or airport operations, direct supervision is not required as long as the AISC holder can ascertain if they leave the 'safe' area.

Aviation related offences

5.17 The offences listed in table 5.1 are considered to be 'aviation related offences' and a term of imprisonment resulting from such an offence disqualifies an individual from holding an ASIC. Additionally, if an applicant has two or more relevant convictions that did not result in imprisonment, with one of these convictions occurring in the last 12 months, they are also ineligible for a card:

Table 5.1: Aviation related offences[9]

Item	Kind of offence
1	An offence involving dishonesty
2	An offence involving violence or a threat of violence
3	An offence involving intentional damage to property or a threat of damage to property
4	An offence constituted by the production, possession, supply, import or export of a substance that is: (a) a narcotic substance within the meaning of the *Customs Act 1901*; or (b) a drug, within the meaning of: (i) regulation 10 of the *Customs (Prohibited Exports) Regulations 1958*; or (ii) regulation 5 of the *Customs (Prohibited Imports) Regulations 1956*
5	An offence, of a kind dealt with in Part II of the *Crimes Act 1914*, against the Government of: (a) the Commonwealth or a State or Territory; or (b) a country or part of a country other than Australia *Note: This includes offences such as Treachery and Sabotage*
6	An offence against Part 2 of the *Crimes (Aviation) Act 1991* *Note: This includes a range of offences, including hijacking, destruction of an aircraft and damage to airport facilities*
7	An offence against Part 5.3 of the *Criminal Code* *Note: Part 5.3 refers to terrorism offences*
8	An offence constituted by the production, possession, supply, import or export of explosives or explosive devices

9 Aviation Transport Security Regulations 2005, ss. 6.01; notes added by committee.

Features of the MSIC scheme

5.18 The MSIC and ASIC schemes differ in a number of ways. There is only one class of MSIC, which can be issued on a permanent (four years) or temporary basis.

5.19 Temporary cards can be issued in one of three circumstances: 1) To the holder of a permanent card if it has been lost, damaged or stolen. 2) To an individual who has been approved for a permanent card, but the issuance of the card has been delayed, and 3) Prior to the completion of a background check, with the Department of Infrastructure and Transport's approval.

5.20 In most cases, the issuing body may determine the duration of the temporary card's validity. As with the ASIC, the MSIC card is not necessarily an access card. However, some issuing bodies combine the port access card with the MSIC. Cards issued by these bodies therefore double as both an MSIC and an access swipe card.

5.21 A visitor who does not hold an MSIC may access secure port areas if escorted by the holder of an MSIC. They do not require an MSIC of their own, although they would presumably still need to respect the private port operator's security arrangements. There are no Visitor Identification Cards in the maritime scheme - these are unique to the aviation sector.

Maritime related offences

5.22 In January 2010, the Minister for Infrastructure, Transport, Regional Development and Local Government announced changes to the MSIC scheme. These changes, which became active in December 2010, included increasing the number of applicable criminal offences from 137 to 298, expanding the list to cover additional matters such as murder, unlawful activity relating to explosives, threatening an airport, kidnapping and bribery.[10]

5.23 The amended list of offences appears below. Simply being convicted for an offence in Part 1 is enough for disqualification, while offences in Part 2 must result in a sentence of imprisonment. Disqualified individuals may appeal to Department of Infrastructure and Transport, with the decision reviewable by the Administrative Appeals Tribunal.

10 AGD, answer to question on notice, 17 February 2011 (received 18 March).

Table 5.2: Maritime Related Offences[11]

Part 1 Disqualifying offences

Item	Matter
1.1	terrorism
1.2	treason, sedition, espionage or selling national secret
1.3	weapon of mass destruction
1.4	hijacking or destruction of an aircraft, vessel or offshore facility

Part 2 Other maritime-security-relevant offences

Item	Matter
2.1	armed attack relating to aircraft, airport, vessel, port or offshore facility
2.2	unlawful interference with maritime transport, offshore facility or aviation
2.3	threat to endanger aircraft, airport, vessel or port
2.4	theft of aircraft or vessel
2.5	piracy
2.6	assassination, murder, attempted murder or manslaughter
2.7	threat to murder
2.8	aggravated assault including the following, whether or not the assault results in injury: • grievous bodily harm • actual bodily harm • torture • wounding • aggravated sexual assault • assault with use of weapon • assault in company
2.9	kidnap
2.10	hostage-taking, deprivation of liberty or false imprisonment
2.11	people smuggling or people trafficking
2.12	racial hatred or racial vilification
2.13	affray or riot
2.14	arson or sabotage
2.15	threat to cause fire or explosion

11 Maritime Transport and Offshore Facilities Security Regulations 2003, Schedule 1.

Item	Matter
2.16	unlawful activity relating to weapons, firearms or explosives (not including weapons of mass destruction)
2.17	armed robbery
2.18	destruction of or damage to property belonging to the Commonwealth
2.19	threat to destroy or damage property belonging to the Commonwealth
2.20	hinder or resist government officer concerned with national security
2.21	bribery or corruption
2.22	extortion, blackmail or racketeering
2.23	money laundering
2.24	false testimony, perjury or subverting the course of justice
2.25	forgery or fraud, including identity fraud
2.26	supply false documentation to get a weapons, explosives or vehicle licence
2.27	unlawful activity relating to passports or visas
2.28	impersonate, misrepresent or falsely advertise a profession or professional status
2.29	deceptive business practice
2.30	import, export, supply, manufacture or cultivate illegal drug or controlled substance
2.31	permit premises to be used for taking, selling or distributing illegal drugs or controlled substances
2.32	conspiracy to commit an offence related to a matter mentioned in items 1.1 to 1.4 and 2.1 to 2.31.

5.24 Further changes introduced in 2010 included reducing the validity period of an MSIC from five years to four with a new requirement for a background check every two years. It also became an offence for a cardholder to fail to advise an issuing body of a conviction for a relevant offence, which may constitute grounds for disqualification.[12]

GHD Report

5.25 These changes, particularly the expansion of relevant offences, were in part the result of a review commissioned by the then Department of Infrastructure, Transport, Regional Development and Local Government in 2009. The consulting firm GHD was engaged to assess the MSIC eligibility criteria and reported in August 2009. As described by Mr Steve Dreezer, OTS:

12 AGD, answer to question on notice, 17 February 2011 (received 18 March).

> The GHD report was part of an extensive departmental review of the Maritime Security Identification Card with industry stakeholders and government agencies. On 29 January, following that extensive review, the Minister for Infrastructure and Transport announced a number of arrangements to strengthen the MSIC scheme.[13]

5.26 In addition to expanding the list of relevant offences, other major recommendations in the GHD report included:

- that consideration be given to including serious convictions resulting in custodial orders imposed by lower courts and all orders (custodial and non-custodial) imposed by higher courts;
- that the Department of Infrastructure further explore the use of criminal intelligence in support of MSIC eligibility determinations; and
- the potential for criminal career information to inform the Secretary's decision in MSIC application appeals.[14]

5.27 Many of the issues raised in the GHD report are addressed below.

ANAO Performance Audit

5.28 The Australian National Audit Office (ANAO) conducted a performance audit of the ASIC and MSIC schemes, tabling the audit report in May 2011. The objective of the audit was to assess the effectiveness of the Department of Infrastructure and Transport's and the Attorney-General's Department's management of the schemes.[15]

5.29 The ANAO made three recommendations, broadly relating to governance arrangements, the issuing process, management of information and compliance activities.

5.30 Firstly, it recommended that OTS review the risks arising from the administrative practices of issuing bodies, particularly in the issuing and manufacture of cards, and evidence of the confirmation of an applicant's identity. It was further recommended that this review be used to assess whether the current arrangements provide an appropriate level of assurance that the scheme's requirements are being met.[16]

---

13 Mr Steve Dreezer, Office of Transport Security, *Committee Hansard*, 18 February 2011, p. 37.

14 Department of Infrastructure, Transport, Regional Development and Local Government, Assessment of Maritime Security Identification Card (MSIC) Eligibility Criteria, Executive Summary, pp 5–8, http://www.theage.com.au/ed_docs/MSIC_Eligibility_Criteria_Part1.pdf (accessed 19 April 2011.

15 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 14.

16 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 24.

5.31 Secondly, the ANAO recommended that in order to provide assurance and improve the outcomes of its compliance activities, OTS should increase the use of information obtained from its audit, inspection and stakeholder programs to focus future compliance activities on areas that represent the greatest security risk. Additionally, it was recommended that OTS capture and share elements of better practice identified through their compliance activity with industry participants.[17]

5.32 Finally, the report recommended that, following implementation of revised visitor management regulations (discussed later in this chapter), OTS should monitor the actual usage of visitor identification cards at security controlled airports and use this information to inform ongoing development of the ASIC scheme and compliance activities.[18]

5.33 The committee supports the recommendations made by ANAO and notes that the Department of Infrastructure and Transport agreed to all three. The committee has used the audit report's findings to support the committee's own analysis below.

Issues with the ASIC and MSIC schemes

5.34 At the time of introduction, the ASIC and MSIC schemes were focussed on preventing terrorist attacks rather than serious and organised crime. Much of the evidence provided to the committee deals with the central issue of whether to extend the schemes to the prevention of non-terrorism related crime, including drug smuggling, tariff avoidance, money laundering and theft.

Expansion of the MSIC and ASIC to combat serious and organised crime

5.35 As discussed in Chapter 2, the committee is of the view that the legislation underpinning the Commonwealth approach to security in the aviation and maritime sectors should be extended to protect against the threat of exploitation by serious and organised crime. This would also require the extension of the MSIC and ASIC schemes to protect against infiltration of the respective workforces by serious and organised criminal networks.

5.36 The Australian Crime Commission informed the committee that the counterterrorism focus of the ASIC and MSIC schemes meant that organised crime groups were able to successfully exploit vulnerabilities in the aviation and maritime environments. As Mrs Karen Harfield, ACC, explained:

> In particular, ACC findings revealed that because the ASIC and MSIC regime was never originally designed to harden the environment against serious organised crime, but rather focus on national security threats in

17 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 24.

18 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 25.

> those environments, these groups have exploited gaps, weaknesses and inconsistencies in the application of the regimes. However, we are also cognisant of the intertwined nature of border security and criminality.[19]

5.37 The Maritime Union of Australia was deeply concerned by the potential for expanding the remit of the MSIC scheme to target infiltration by organised criminal networks. The MUA considered that the MSIC had become a 'right to work' card, in that employment on the waterfront was conditional on holding an MSIC. Mr Dean Summers, MUA, made clear that the tightening of the eligibility criteria for an MSIC was a serious issue for the union.

> I just want to stress at this stage that the Maritime Union in particular, and different from all the other unions, considers that the MSIC has become a right-to-work card in that if we cannot have an MSIC, our members—about 12,000—unlike truck drivers, rail workers and some port workers, we cannot go to another area of work. That takes away our ability to earn money to have a job. So we have labelled it a right-to-work card.[20]

5.38 Mr Summers further informed the committee that the MUA had cooperated with the government in developing the current MSIC eligibility criteria out of a shared concern for the need to prevent terrorism, stating:

> We debated with industry many times for robust formats: how deep those background checks should go into workers' backgrounds given the nature of our work, the responsibilities, particularly in the offshore oil and gas and on the waterfront. It protects our borders. We know that we arrived at a position where we were confident—and at the time the government was confident—that checked workers' backgrounds to such a degree that they were no threat to maritime security in any of those areas of work.[21]

5.39 Ports Australia also expressed reservations about extending the MSIC scheme to cover serious and organised crime, stating:

> Our position is that we have some reservations about extending the reach of MSIC to address serious crime. We have had concerns in the past that there has been some perception that port authorities are central to crime-fighting efforts. We use our best endeavours, of course, to cooperate with the relevant agencies, but our core business is the facilitation of trade. We leave it to others to determine an appropriate regime to address serious crime, which is now well and truly out there in the public arena.[22]

5.40 The committee accepts that the extension of the schemes to include serious and organised criminality carries attendant issues, but remains of the opinion that the significant risk posed by criminal infiltration of aviation and maritime workforces

---

19 Mrs Karen Harfield, ACC, *Committee Hansard*, 17 February 2011, p. 8.

20 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 2.

21 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 2.

22 Mr David Anderson, Ports Australia, *Committee Hansard*, 18 February 2010, p. 49.

warrants such action. Accordingly, the committee supports an extension of the scheme to combat serious and organised crime, in line with its previous recommendation of an extension of the focus of ATSA and MTOFSA. Specific mechanisms to do so include the use of criminal intelligence and reviewing the list of relevant offences under each scheme and are canvassed below.

Scope of relevant offences

5.41 A key feature of the ASIC and MSIC schemes is limitation of the criminal history assessment to 'relevant' offences, listed above. These relevant offence lists were developed with the need to prevent terrorism in mind. As a result, several witnesses have suggested the inclusion of further offences that relate to broader criminality, in order to reorient the schemes towards preventing crime in both sectors.

5.42 The increased number of maritime-related offences announced in January 2010 (described previously in this chapter) represents some movement towards such a broadening of the MSIC scheme, although the focus of those offences remains terrorism.

5.43 Airservices Australia (ASA) noted that the current definition of aviation related offence could be reviewed to ensure that all offences which could pose a future risk to aviation security are actually discovered at the screening stage. Specifically, ASA noted that the current definition does not include offences involving firearms and other weapons and offences relating to involvement with a serious criminal organisation.[23]

5.44 Rather than recommend the addition of any further offences directly, the committee recommends that the Attorney-General's Department, in consultation with the Australian Crime Commission, review the list of relevant offences under each scheme to assess whether any further offences related to serious and organised crime need to be included in the regulations if the scheme is to prevent serious and organised crime.

Recommendation 14

5.45 The committee recommends that the Attorney-General's Department, in consultation with the Australian Crime Commission, reviews the list of relevant security offences under the ASIC and MSIC schemes to assess whether any further offences are required in order to effectively extend those schemes to protect the aviation and maritime sectors against the threat of infiltration by serious and organised criminal networks.

23 AirServices Australia, *Submission 4*, p. 5.

Use of criminal intelligence

5.46 In addition to ensuring that the relevant offences list accurately documents offences relating to organised crime, the use of criminal intelligence held by law enforcement agencies should be used to prevent known criminal figures from holding ASICs or MSICs.

5.47 The current security assessment by ASIO is directly relevant to supporting national security. However, a number of witnesses were concerned that there was no equivalent use of criminal intelligence that would assist in resisting criminal infiltration of airports. For example, Sydney Airport Corporation Ltd (SACL) noted that (in the context of NSW), the background check could refer to supporting information such as past decisions about whether an individual was a fit and proper person to own a firearm, or to hold a security license.[24]

5.48 Similarly, the Australian Transaction Reports and Analysis Centre (AUSTRAC) suggested in its submission to the committee that the use of criminal intelligence would assist in determining whether an individual was 'fit and proper' to hold a card. In addition to information held by agencies such as the ACC, this also included financial information held by AUSTRAC.[25]

5.49 The AFPA were in favour of the use of criminal intelligence in determining eligibility for an ASIC or MSIC, using a 'fit and proper person' test auspiced by the AFP Commissioner.[26]

5.50 Qantas was also in favour of the use of criminal intelligence in establishing eligibility for the ASIC in particular. As Mr Stephen Jackson, Head of Security and Facilitation, Qantas Airways Ltd, commented:

> To assist in combating the threat posed by trusted insiders, Qantas has held a longstanding view that a strengthened aviation security identification card and ASIC regime should include a criminal intelligence check as an additional dimension to the existing range of background checks—as you know, criminal history, conviction, citizenship, national security or [Politically Motivated Violence] checks are conducted by ASIO—together with a process to deliver live checking of a person's criminal convictions against their ongoing eligibility to continue to hold an ASIC.[27]

5.51 Mr Richard Janeczko, a private consultant, was also for the use of criminal intelligence:

> I believe that people who are working in sensitive areas do need to have quite strong checks carried out. I am a strong supporter because too often in

---

24 Mr Rodney Gilmour, SACL, *Committee Hansard*, 18 February 2010, p. 15.

25 Mr Schmidt, AUSTRAC, *Committee Hansard*, 18 February 2010, p. 26.

26 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 28.

27 Mr Stephen Jackson, Qantas, *Committee Hansard*, 18 February 2011, p. 26.

> the business that I have been in we come across people who really should not be working in that environment—for example, people with criminal records. So I think that quite strong checks should be carried out... I think people who work in that area must understand they are working in a privileged area and if public security is involved, as well as organised crime, they should be willing to provide that information.[28]

5.52 However, several witnesses voiced significant concern about the potential abuse of criminal intelligence. The main arguments against the use of criminal intelligence included doubts regarding the veracity of such intelligence, the possible inability to challenge an adverse finding if the process or intelligence remains confidential or due to cost, and the infringement of human rights such a scheme could entail.

5.53 For example, the Transport Workers Union (TWU) questioned the ability to responsibly use criminal intelligence, which was not necessarily robust, highlighting the case of Dr Mohamed Haneef. As Mr Anthony Sheldon, TWU stated:

> The use of criminal intelligence must be balanced between the human rights of workers—the right of privacy, the right to appeal decisions and the right to know information that is being used to make decisions about your livelihood—and the need to protect against the employment of terrorists or organised crime figures. Let us remember that Australia is not a secret police state but an open, liberal democracy. Police intelligence can be wrong—and often is—as it consists of anonymous tip-offs, rumours, associations and the like; it is not court tested evidence that is used to prosecute someone for an offence.[29]

5.54 Furthermore, the TWU was concerned about the potential for false criminal intelligence to be used against union activists to deny them access to airport and port facilities.[30]

5.55 The TWU also argued that a transport worker that lost their employment due to an adverse finding relying on criminal intelligence could not be expected to mount a lengthy and expensive legal challenge against potentially secret information. As Mr Sheldon noted:

> [A]ny system would have to [have] included the right of an appeal to an independent and low-cost tribunal with all material being used to make decisions being able to be seen and challenged by the transport worker. The presumption should be in favour of the transport worker, with the government required to prove that there is currently a risk.[31]

---

28 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 16.

29 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 52.

30 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 51.

31 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 53.

5.56 The Maritime Union of Australia, Australian Workers Union, Rail, Tram and Bus Union, Australian Maritime Officers Union and the International Workers Federation provided a joint submission highlighting concerns that use of criminal intelligence would infringe on worker's rights. The submitting unions were concerned that it may be used against union officials and questioned the reliability of criminal intelligence. Furthermore, the organisation was of the opinion that punishing workers who may have offended in the past was unfair and amounted to 'double jeopardy'.

5.57 Appearing before the committee at a hearing, Mr Dean Summers, MUA, made two main arguments:

> The first is the double jeopardy question. People who have offended and who have paid for their crime and done their time and, hopefully, been rehabilitated through the Australian system, should be allowed, therefore, to go back into a workforce.

5.58 He also argued that criminal intelligence was notoriously unreliable and should not be the basis for depriving someone of an employment opportunity.[32]

5.59 The Australian Services Union noted the importance of balancing the need for security measures with both the civil liberties of workers and the practicalities of workers doing their jobs.[33]

5.60 The Australian Federal Police explained that a number of issues could make the use of criminal intelligence difficult. Mr Phelan, Deputy Commissioner, explained that a system that required intelligence to be made public may prevent its actual use, stating:

> Not the least of those is that intelligence is intelligence; it is not evidence. So if we are put to the test with some of that information, which I would imagine would be the case, and if we are defending those cases, we would have to be very discerning about giving up our sources or where the particular intelligence came from. That could in fact lead us to withdraw from actually defending a particular case that might be against us.[34]

5.61 Similarly, the establishment of a process by which criminal intelligence could be used would involve a number of difficult decisions regarding the process design. As Mr Phelan noted:

> [W]hat intelligence do we use? What threshold do we use? Where do you go to get that intelligence? Do you go to each and every one of the state police agencies, the Federal Police, the ACC, ASIC, the ATO, Customs; all the various other law enforcement agencies, like the New South Wales Crime Commission and the various corruption commissions that exist?

---

32 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 9,

33 ASU, S*ubmission 7*, p. 3.

34 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 39.

> There is myriad intelligence held that is not evidence based, and it is important to work out where you go. Even then, if we were to say that intelligence was appropriate, what level do we set that within an agency? What sort of intelligence? How robust is that information? How truthful is that information? How historic is that information? And so on and so forth. So there are a lot of vulnerabilities in using intelligence, and that is why, from our perspective, we are not fully supportive of using intelligence to determine one's ability to get an MSIC card.[35]

5.62 Of particular concern in such a scheme was the balance struck between the relevance and robustness of a particular piece of intelligence. As Mr Phelan explained:

> ...what if you had something that was F6, which is information that has not been tested and the accuracy of which is unknown, but it is a very important aspect—it might say, 'This person is a drug importer'—and then you might have A1 intelligence that says that the person is in a much lesser position, for instance they have stolen something or other. Using the Admiralty Scale, based upon the type of intelligence rather than its reliability, is difficult, because the most important intelligence may be in your F6 type arrangement.[36]

5.63 The Admiralty scale refers to a two-character scale used to assess intelligence. Information is ranked from A to F in terms of the reliability of a source and 1 to 6 in terms of credibility, based on likelihood and corroboration by other sources.

5.64 The committee accepts the issues raised by witnesses regarding the use of criminal intelligence and considers that any potential scheme would require careful construction. Nevertheless, the committee is aware that a number of individuals that are strongly suspected to have been involved in criminal activity or have strong associations with known organised criminal networks currently hold ASICs and MSICs.

5.65 The committee is of the opinion that these individuals constitute a serious threat due to their ability to exploit vulnerabilities within the aviation and maritime sectors by acting as trusted insiders for organised criminal networks. The committee considers that the inability to revoke the ASICs and MSICs of these individuals is unacceptable and therefore is of the view that the use of criminal intelligence be incorporated into the ASIC and MSIC schemes.

5.66 The number of individuals affected is not likely to be high. The vast majority of aviation and maritime workers are not involved with serious and organised crime. The ACC informed the committee that as at May 2011, less than three per cent of

---

35 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, pp 39–40.

36 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 41.

individuals holding an ASIC or MSIC were identified in ACC intelligence holdings.[37] Furthermore, only some of those within this three per cent of cardholders would potentially be deprived of a card. As the ACC explained:

> There are a range of people who are identified on ACC systems who are not involved in any behaviour that would prohibit them obtaining an ASIC or MSIC. For instance, an associate of a person of interest with no criminal involvement or an individual with past criminal history that no longer has a bearing on their ability to obtain an ASIC or MSIC are included in ACC intelligence holdings.[38]

5.67 The committee is not of the view that a criminal intelligence assessment should be part of the application process coordinated by Auscheck. This would most likely delay the issuing of ASICs and MSICs, potentially exacerbating the problem of overreliance on visitor provisions under both schemes.

5.68 Instead, the committee envisions a model by which a suitable law enforcement agency, to be selected by the Attorney-General's Department, would be given the authority to make a determination to revoke an ASIC or MSIC on the strength of compelling criminal intelligence.

5.69 The committee is of the view that the ACC is the most logical agency to be given responsibility for making such a determination. In practice, other law enforcement agencies, including the AFP, Customs and state and territory police could seek a determination to revoke a card by approaching the ACC with specific intelligence about a cardholder.

5.70 The committee is also of the view that law enforcement agencies would not be required to publicly reveal the criminal intelligence used to make a determination. To do so would effectively prevent law enforcement agencies from seeking a determination in most cases, rendering the provision mostly useless.

5.71 However, the committee is aware that the use of confidential criminal intelligence to make such a determination requires a robust appeal mechanism to ensure that the power does not become subject to abuse. For this reason, the committee suggests the development of a public set of criteria that would be used in order to make the determination and the provision of an independent arbiter that would review determinations made under the scheme to ensure adherence to the agreed criteria.

37 ACC, answer to written question on notice, 9 May 2011 (received 25 May 2011).

38 ACC, answer to written question on notice, 9 May 2011 (received 25 May 2011).

Recommendation 15

5.72 The committee recommends that the Attorney-General's Department arrange for a suitable law enforcement agency to be given the power to revoke an Aviation Security Identification Card or Maritime Security Identification Card if it is determined that a cardholder is not a fit and proper person to hold a card on the basis of compelling criminal intelligence.

Imprisonment criteria

5.73 As noted above in the description of the ASIC and MSIC schemes, in most cases an applicant must have been imprisoned for a relevant offence before they are precluded from holding an ASIC or MSIC. Some witnesses see this as a weakness of the scheme, maintaining that a conviction that does not lead to imprisonment could warrant disqualification.

5.74 A related issue was the time delay between a cardholder being charged and convicted for a relevant offence. Currently, cardholders continue to hold their ASIC or MSIC until the point of conviction, despite the potential security risk posed by the applicant. AusCheck noted that a suspension mechanism could provide a solution, stating:[39]

> We can also look at some of the issues around criminal convictions and ASICs and MSICs. I know that there is a presumption of innocence, but perhaps when we charge someone for something and they go before the courts there should be a mechanism there for suspension or something similar to that. At the moment, they do not lose their ASIC cards because of pending criminal action. It is only [upon] a conviction that they do so. [40]

5.75 The committee notes that the majority of offences that would indicate possible involvement with serious and organised crime would attract a term of imprisonment. However, the committee is concerned that as the requirements stand, the imprisonment requirement constitutes a potential loophole. The committee would therefore prefer to see the provision within the ASIC scheme be duplicated in the MSIC scheme. If an applicant has two or more relevant convictions that did not result in imprisonment, with one of these convictions occurring in the last 12 months, they would also ineligible for a card.

39 Mr Geoff McDonald, AGD, *Committee Hansard*, 17 February 2011, p. 20.

40 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 39.

Recommendation 16

5.76 The committee recommends that the MSIC eligibility criteria be harmonised with that of the ASIC scheme so as to make two or more convictions of an individual for maritime security relevant offences grounds for disqualification if one of those convictions occurred in the 12 months prior to an application, regardless of whether either conviction led to a term of imprisonment.

Visitor provisions

5.77 The committee heard that the visitor provisions under both the MSIC and ASIC schemes were potential vulnerabilities. Within the ASIC scheme, visitors must be provided a Visitor Identification Card and supervised by an ASIC cardholder. Mr Stephen Jackson, Qantas, noted the potential for exploitation, stating:

> There are some people who use the VIC regime to step around the ASIC regime. Mainly, in my experience, that is from being lazy, but it still does present an environment that those who might want to engage in criminal behaviour could exploit. That is why we are absolutely behind the government in strengthening the regime and moving to a significant reduction in ASIC-issuing bodies—and likewise with the visitor identification card regime. There are amendments underway for the VIC regime to be strengthened quite considerably, which we fully support.[41]

5.78 Mr Grant Woods, SACL, informed the committee that the Visitor Identity Card was necessary to ensure the day to day operation of the airport, stating:

> The visitor pass system is a very important part of airport life. If we have a failure of a pavement and we have to get a contractor in to dig it out and fill it to make the airport safe, it is very hard to wait for five or six days for an application to go through to get that done. So the visitors' passes are there for normal business at an airport to continue, but in a very controlled sense. We would issue a visitor pass more frequently on a day-to-day basis as the need may occur, and there may be a number of times where a visitor may be required to be at the airport for three or four days.[42]

5.79 The processing time for an ASIC has resulted in a practice whereby some companies rely on VICs for a significant proportion of their workforce. The TWU informed the committee that they were aware of contract staff being issued visitor cards for extended periods of time, as explained by Mr Anthony Sheldon:

> A large proportion of contractors who work at Australian airports are labour hire employees. These employees work in secure areas of the airport prior to the completion of their background checks. They are often covered through a temporary visa pass while their application is being processed. These employees could have any number of infringements that render them

41 Mr Stephen Jackson, Qantas, *Committee Hansard*, 18 February 2011, p. 31.

42 Mr Grant Woods, SACL, *Committee Hansard*, 18 February 2010, p. 16.

> unsuitable for security clearances, but under the current system the authorities do not know for two months at best, and we are aware of circumstances where people have not been suitably audited for up to six months. It is for these reasons that the TWU submission recommends that the use of visitor identification cards for more than one month in a year be prohibited.[43]

5.80 The TWU informed the committee that their investigations suggested that up to 25 per cent of security guards at Sydney Airport were using Visitor Identification Cards during peak periods, while their application for an ASIC was processed.[44]

5.81 The substantial use of VICs by individuals as a means to regularly access secure areas of an airport was confirmed by Australian National Audit Office (ANAO) analysis. While the ANAO was not able to determine the actual number of VICs issued annually, it found that at one delivery gate at a major airport, around 40 000 VICs were issued in 2009–10. Ninety per cent of these VICs were issued to individuals who had multiple visits.[45]

5.82 The ANAO report also noted that OTS regularly identifies examples of non-compliance with ASIC requirements, including the lack of supervision of VIC holders.[46]

5.83 The Office of Transport Security informed the committee that the Government is currently considering changes to the VIC as a result of the aviation white paper process. Mr Paul Retter, OTS, stated:

> The government announced in the aviation white paper response that we would include additional measures to enhance visitor processes so that there were greater controls on who had access. Those arrangements have been the subject of extensive negotiation and consultation with industry since they were announced. I am pleased to report that the proposed arrangements are currently with the minister for his concurrence. Presuming that he is happy with those enhanced arrangements, we anticipate they will be issued in 2011.[47]

5.84 Within the MSIC scheme, visitors do not require any card, but must be escorted by an MSIC cardholder. While convenient, this is a potential vulnerability, as noted by Mr Dean Summers, MUA, who stated:

---

43 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 51.

44 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 56.

45 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 22.

46 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 21.

47 Mr Paul Retter, Department of Infrastructure and Transport, *Committee Hansard*, 18 February 2011, p. 35.

> I have heard that people will lend themselves and their cards to sit in the cabin and go through a terminal, so that somebody else inside of the cab has an MSIC. That in itself is a bit of a problem, if somebody is sitting out the front with a shingle over their heads saying 'MSIC for hire on an hourly basis' and there is no relationship between the driver and the card.[48]

5.85 The committee is concerned by the substantial vulnerability arising from the visitor provisions for both the ASIC and MSIC schemes. The committee considers that the VIC scheme requires reform, and encourages the government to reduce the duration an individual can continue to access secure areas using a VIC as part of the aviation white paper process currently underway.

Coverage of the scheme

5.86 As noted in Chapter 2, aviation and maritime security is not just about airports and ports, and needs to address vulnerabilities across the aviation and maritime sectors. Criminal organisations exploit the same supply chains used by legitimate business for illicit purposes. The security response must therefore address the supply chain in total rather than just one point along the transport route.

5.87 As noted by Mr Dean Summers, MUA, the criminal exploitation of the maritime sector involves more people than just waterfront workers. Senior management, company human resource sections and other elements of the maritime industry working outside of the port security area are all in a position to corrupt the maritime sector. As Mr Summers explained:

> Some are responsible for the placing of ships and cargoes and for the coordination of which ships go to which berths, which trains go to which berths and which trucks go to which departments and depots. They are all things where effective control of cargoes and manpower on the waterfront and on the offshore oil and gas rigs are completely unchecked. We think that is a pretty obvious gap in security. If it is good enough to background check and scrutinise those workers at the coalface then surely we have to look back a few steps and have the same level of scrutiny for those people who have effective control of all those issues I just mentioned.[49]

5.88 Foreign crews, including those on flag of convenience vessels, may be subject to less stringent background inquiry, yet could act on behalf of serious and organised criminal networks, as indicated in an example provided by Mr Summers:

> We are worried that Australian seafarers must undergo these background checks while foreign seafarers—working on the same trade sometimes, on coastal shipping permits—need a very cursory background check. These are people from countries that are very difficult to background-check, such as Pakistan and the Philippines. Those people can come and work on our coast, on ships that have replaced Australian ships, on what and the

48 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 7.

49 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 3.

> international industry have labelled 'flag-of-convenience vessels', which effectively are deregulated. These vessels are also responsible for carrying cargoes like explosive-grade ammonium nitrate around the Australian coast. While the production, storage and transport are highly scrutinised and background-checked, controlled and regulated, as soon as it comes to an Australian wharf and is handed over to an FOC ship it is completely deregulated and usually, on every occasion that we know of, to the lowest bidder using the cheapest crews and, on many occasions, substandard ships.[50]

5.89 The extremely low pay and poor working conditions that may exist on flag of convenience vessels provides a strong incentive for corruption of that particular workforce, as argued by Mr Summers, who stated:

> Yesterday I made some remarks to the Maritime Security Forum that I was aware that last week there was a cattle vessel in Fremantle with 80 crew on board, which is a very big crew.Most of them were Pakistanis and they were employed by a dodgy crewing agent in Pakistan who was paying them $300 a month. The ITF was successful in getting the company to sign an agreement for $1,000 a month for each of these seafarers, which is still very low by the international standard. But we found subsequently that the crew had to pay three months wages just in order to secure a job. So they had to sign their first three months wages away, and they were being underpaid by $600 a month. So they were back to their $300-odd a month. These people are very vulnerable. These people are coming to and from Australian ports, being paid, being intimidated, being bullied and being forced to sign things that they would not otherwise sign. Subsequently, we are told, at least three people jumped ship.[51]
>
> Last week I saw the crew of a car vessel, who had not been paid for four months. That vessel was trading around Australia delivering luxury cars. If these people are not ripe for the picking by evildoers, then I do not know who is.[52]

5.90 Mr Summers explained that the shipping industry was essentially broken down into two parts: international shipping and a coastal industry. While the Commonwealth Government is moving to support the coastal industry with secured, background checked, regulated Australian ships and crews, the international market, particularly under flag-of-convenience operators was subject to less rigorous regulation.[53]

5.91 Mr Summers noted that the Australian Maritime Safety Authority had a system for profiling ships of greatest risk in terms of safety. He further surmised that

---

50 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 3.

51 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 5.

52 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 5.

53 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 6.

the risk profile of flag-of-convenience vessels, particularly those with the lowest paid crew, could be used to inform screening for criminal activity by Customs and other law enforcement agencies.[54]

> If they are coming to Australian shores and ports they should be the subject of Australian criminal investigations. I have witnessed seafarers being beaten and had a terrible time trying to get police assistance because they are unsure of their jurisdiction of a foreign flagged ship. On a Panamanian or Mongolian flagged vessel, who has jurisdiction? It would bear closer investigation and we would be happy to participate.[55]

5.92 Additionally, cargo and containers leave the port environment destined for a number of bonded stores, unpacking facilities and other workplaces that are not part of maritime security legislation.

> Finally, the Trojan horse conditions: the stuffing and unstuffing of containers done in depots often outside maritime security regulated zones. These people are casualised workers with no background checking at all, deregulated and what we would label as 'uncontrolled'. From those depots, the customs seals are applied onto the containers themselves. You do not have to have any background check to apply a seal. You just buy one and put it on a container. Then the container is completely locked and secured all the way through maritime security regulated zones onto ships and to a foreign birth and possibly to a depot that is outside another country's maritime security regulated zone.[56]
>
> We know this is a largely casualised area, so low-paid and non-organised workers come in there to open the containers, stuff them or the goods are sent to a container yard because sometimes you might not have enough goods to send in one container so the company will organise to send a whole lot of people's stuff in one container. These people stuff those containers and then are responsible to put a security seal on that container and send it into a security regulated zone.[57]

5.93 The committee agrees with Mr Summer's concerns and is of the opinion that the coverage of the ASIC and MSIC be extended to include other areas of the aviation and maritime sectors.

---

54 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 6.

55 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 6.

56 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 4.

57 Mr Dean Summers, MUA, *Committee Hansard*, 18 February 2011, p. 13.

Recommendation 17

5.94 The committee recommends the expansion of the coverage of the ASIC and MSIC schemes to capture a greater part of the overall supply chain, including some or all of the following:

- **staff at cargo unpacking and stuff-unstuff facilities;**
- **transport workers involved in the transmission of cargo between ports, airports and other parts of the logistical chain;**
- **customs brokers that do not access port facilities; and**
- **human resource staff and management at companies with employees that currently must hold ASICs or MSICs.**

Realtime checking

5.95 A number of witnesses before the committee were concerned that under the current scheme, cardholders were only assessed once every two years. This potentially meant that relevant offending would not be detected in a timely fashion, undermining the objective of the scheme.

5.96 Mr Grant Woods, Sydney Airports Corporation Ltd (SACL), expressed a preference for a mechanism by which notification of relevant offences could occur in a more instantaneous fashion, stating:

> In the period between the issue—that two-year period—we are looking for the law enforcement agencies to advise us of any criminal behaviour or behaviour that would be against the criteria for issue when that becomes known to the law enforcement agencies themselves. So, for example, when we issue a card to a person we do not have any visibility of that person for another two years. If they commit a crime within the first three months of the card being issued we would be looking to the state police or the Federal Police to understand that there is a person out on the airfield who now contravenes the issuing criteria and to advise us accordingly so that we can take action. We think that is a very important part of that process.[58]

5.97 Since SACL appeared before the committee in February 2010, some changes have been made, including making it an offence for a cardholder to fail to notify an issuing body if they have been convicted of a relevant offence.[59]

5.98 The committee does see value in the introduction of a 'livechecking' arrangement, whereby assessment of an ASIC or MSIC cardholder's eligibility occurs

---

58 Mr Grant Woods, SACL, *Committee Hansard*, 18 February 2010, pp 14–15.

59 Department of Infrastructure and Transport, 'Fact Sheet: ASIC Enhancements 1 December 2010', http://www.infrastructure.gov.au/transport/security/aviation/factsheet/asic_enhancements.aspx (accessed 17 May 2011).

on an ongoing basis rather than at two year intervals. This would enable relevant information to be used in a timely fashion.

5.99 CrimTrac advised that such a scheme, involving ongoing sharing of information, was likely to raise privacy issues in addition to a significant upgrading of the current database:

> Regarding the issues about the holding of the information on the applicants of the ASIC and the MSIC, if it were accepted as a matter of policy that CrimTrac would, for example, do continuous checking based on parameters that were provided, there would of course be a necessity to have access to that information on a continuous basis; that is implicit in the ability. By extension, you would then need to deal with the issue of who has access to that data... Implicit in that, there are then the questions of privacy, the rules of access and what the information can be used for.[60]

5.100 CrimTrac is currently investigating the feasibility of supplying continuous updates on criminal records, helping to reduce the system's current reliance on cardholders self-reporting.[61] However, there are likely to be a number of issues, as noted by the Attorney-General's Department:

> ...the ability of CrimTrac to supply real-time, continuous criminal history information would require high-levels of connectivity between police, law enforcement agencies and stakeholders. This is a significant task under active consideration that will require the joint efforts of relevant State, Territory and Commonwealth agencies and would take time to implement.[62]

5.101 The committee is of the opinion that the introduction of a continuous relevant security offence assessment mechanism is highly desirable and would eliminate a current vulnerability in the scheme.

Recommendation 18

5.102 The committee recommends that Auscheck and CrimTrac work together to develop a database system that enables continual assessment of a cardholder's criminal record in order to ensure that cardholders are disqualified very soon after being convicted of a relevant security offence.

Biometrics

5.103 Another suggestion for improvement of the ASIC and MSIC schemes was the use of biometric information such as fingerprints or facial recognition. Biometric information could serve two purposes. Firstly, it would provide a more robust means

60 Mr Douglas Smith, CrimTrac, *Committee Hansard*, 18 February 2011, p. 51.

61 AGD, *Submission 14*, p. 11.

62 AGD, *Submission 14*, p. 11.

to link cards to cardholders, simplifying database management while, secondly, enabling the use of enhanced access technology at airports and ports.

5.104 As CrimTrac noted, the current name-based system, whereby the identity of cardholders is managed through names, is vulnerable due to difficulties such as spelling and name changes. As Ms Roberta Kennett, CrimTrac explained:

> There have been some conversations around some of the vulnerabilities of name based checking. Some of those have already been mentioned, but, essentially, it is possible for people to change their names and there are complications around matching with names. We need to use a fuzzy logic algorithm to allow us to match names that have, perhaps, been misspelt or are in a different order, or things like that. There have been some early discussions around strengthening that name based checking regime and using biometrics as an identifier to help strengthen that regime.[63]

5.105 Simplifying the management of the system in such a way would therefore simplify the introduction of other ASIC and MSIC improvements, such as the implementation of a continuous criminal record check, recommended above.

5.106 Biometric information could also be used to improve the access security at aviation and maritime security areas. As CrimTrac explained:

> We submit that it would be useful to consider conducting a fingerprint check at [the point of application or card renewal] to ensure that the identity of the person who is presenting themselves is in fact the person who is presenting themselves. It overcomes some of the vulnerabilities in the system, such as names not being matched correctly or documents that have been obtained fraudulently being verified as valid. That was the main thrust of our initial submission. The secondary aspect is to look at the inclusion of a biometric for controlling access to and from the site.[64]

5.107 This secondary aspect is also of interest to the committee, but no doubt would involve a significant additional cost. Mr Geoff McDonald elaborated on this subject, stating:

> Clearly, to make it efficient, it is useful to have electronic scanners and things like that. So implementation of biometrics would involve quite a big capital investment; there is no question about that. And, of course, we have a circumstance where we have to look at the cost-benefit analysis of every national security measure and weigh it against other national security measures. So we have mentioned that. Obviously, there is some work being done in this area. We have no doubt that a fingerprint based scheme would be a better scheme in terms of guaranteeing absolutely that the person you are talking about is that person.[65]

---

63 Ms Roberta Kennett, CrimTrac, *Committee Hansard*, 18 February 2011, p. 51.

64 Ms Theresa van Gessel, CrimTrac, *Committee Hansard*, 18 February 2011, p. 49.

65 Mr Geoff McDonald, AGD, *Committee Hansard*, 17 February 2011, p. 21.

5.108 The use of fingerprint scanners or facial recognition technology could significantly increase the integrity of security, as noted in the previous chapter where the committee recommended that port gates be upgraded to ensure that the holders of card are assessed against the photo on the card – a lower technology version of a true biometric scheme.

5.109 Mr Kim Langton, Chameleon Associates, strongly favoured the introduction of biometric readers to control access to secure areas, stating:

> You really need to know where the card is going. I can take a card and, as long as I look similar to the person who is meant to have it, I can get in whereas with biometrics you are controlling access and egress of the site. Biometrics is the way to go.[66]

5.110 Mr Michael Carmody also expressed support for such a move, stating:

> From its inception the ASIC has been a reasonable albeit fundamentally flawed idea in that the system is about tracking cards, not people. That is the fundamental disconnect in the exercise because what it cannot prevent is the passage of cards or the duplication of cards, and that situation has not changed today... The need to move to more biometric sensitive equipment whereby you actually start tracking people and not necessarily what is hanging around their neck has to be the logical next step.[67]

5.111 CrimTrac noted that the easiest technology to use for the purposes of the ASIC and MSIC schemes would probably involve fingerprints, though it would be possible to use facial recognition technology.

> Certainly from CrimTrac's perspective and a law enforcement perspective, we have a long-established database of fingerprints. Although CrimTrac does not currently run a facial recognition system, facial recognition is growing in popularity, and that is used in some law enforcement agencies and certainly the Passports Office. That is also a proven biometric technology.[68]

5.112 AFPA noted the potential to match facial information using image recognition software in conjunction with existing efforts using drivers licences by CrimTrac, stating:

> It is an important issue. When they were trialling this system in Victoria... they found large numbers of people having numerous drivers licences and this program picked up the duplication of photos. I think in one case one person had multiple drivers licences—a number of 30 to 60. The issue here is that the technology is there. If CrimTrac wants to continue trialling its

66 Mr Kim Langton, Chameleon Associates (Australia), *Committee Hansard*, 18 February 2011, p. 55.

67 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 1.

68 Mr Jeremy Johnson, CrimTrac, *Committee Hansard*, 18 February 2011, p. 49.

> system there is an opportunity here to enhance security by running those old records through a face recognition program.[69]

5.113 The AFPA noted that applicants may object to providing biometric information for a variety of reasons including privacy concerns. However, as they argued, a number of other occupations require the provision of detailed personal information, stating:

> The important thing here is for you to get other clearances for different roles, such as a teacher. There are a number of professions where you have to provide a unique identifier. Surely, on both national security grounds and with regard to organised crime, which now fits within the national security statement, there is a justification to prove the identity of people working in these locations.[70]

5.114 The committee strongly supports the introduction of biometric information to the ASIC and MSIC application process. Initially, such a measure would improve the management of the database making it more efficient and opening other possibilities such as continuous checking. In time, the use of biometric information could also extend to access technology at aviation and maritime security zones.

Recommendation 19

5.115 The committee recommends that use of biometric information, particularly fingerprints, to establish a unique identifier for applicants for the purpose of maintaining an accurate database of cardholders.

Recommendation 20

5.116 The committee recommends that the Australian Government consider the use of biometric information for the purpose of controlling access to security controlled areas in the aviation and maritime sectors.

5.117 The use of biometrics in simplifying database management for the ASIC and MSIC may also help to correct another problem, raised by witnesses such as Mr Stephen McInerney, ASU, who noted that application for card renewals required the resubmission of the same information each time.[71] This onerous application process risks unnecessarily alienating applicants from the security regime. The committee is therefore of the view that the application process should be streamlined in conjunction with the introduction of biometric markers to avoid unnecessarily burdening renewing cardholders.

---

69 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 33.

70 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 35.

71 Mr Stephen McInerney, ASU, *Committee Hansard*, 17 February 2010, pp 9–10.

Sharing of information with other agencies

5.118 AusCheck is currently restricted from providing law enforcement and intelligence agencies, such as the AFP and ASIO, with real-time access to information stored on AusCheck's database. Instead, agencies are provided with information from the database which had been copied onto a CD or in a written document and hand delivered.[72] This is approach is a response to privacy and other concerns.

5.119 The delay represented in such a cumbersome approach inhibits the sharing of useful information. Auscheck is currently exploring the feasibility of establishing an MOU with the AFP to provide information in real time. Though not giving the AFP physical access to the database, the speed with which information can be provided would be significantly improved.[73]

5.120 Mr Geoff McDonald, First Assistant Secretary, AGD, informed the committee that AusCheck received requests for information from the AFP, the ACC and Customs on occasion. In addition, ASIO, AUSTRAC, Centrelink and the Department of Infrastructure and Transport could potentially request information from the AusCheck database.[74] The agencies had to demonstrate that a request for information was for the purpose of law enforcement.[75] Mr McDonald went on to say:

> Clearly, if we had more streamlined systems it might be of more use. However, like the other issues that we have discussed, it would have a technological and resource impact because of which, when weighed up against all the many other things that are going on, the national security space might not get the same priority. If you want to look at an area where there could be improvement, we have just identified one.[76]

5.121 Ms Tamsyn Harvey, noted the importance of secure electronic communications and the ability of agency systems to interact successfully in enabling swift information sharing.[77]

5.122 AUSTRAC informed the committee that broader access to ASIC and MSIC data would assist criminal intelligence agencies to identify possible criminal activity in ports and airports.[78]

5.123 The committee agrees that the accessibility of information held by AusCheck is potentially critical to certain operations. It is therefore supportive of moves to

---

72 AGD, *Submission 14*, p. 13.

73 AGD, *Submission 14*, p. 13.

74 Ms Tamsyn Harvey, AusCheck, *Committee Hansard*, 17 February 2011, p. 23.

75 Mr Geoff McDonald, AGD, *Committee Hansard*, 17 February 2011, p. 22.

76 Mr Geoff McDonald, AGD, *Committee Hansard*, 17 February 2011, p. 23.

77 Ms Tamsyn Harvey, AusCheck, *Committee Hansard*, 17 February 2011, p. 23.

78 AUSTRAC, *Submission 11*, p. 6.

establish MoUs with the AFP and other key law enforcement and intelligence agencies in order to increase the speed with which information can be shared.

Recommendation 21

5.124 The committee recommends that AusCheck establish memoranda of understanding with the Australian Federal Police and other key law enforcement and intelligence agencies in order to allow the timely provision of information held in the AusCheck database to those agencies.

Issuing bodies

5.125 Although AusCheck centrally manages the actual background checking process, there are currently a large number of organisations that have been authorised to issue ASICs and MSICs. There are approximately 22 of these issuing bodies in the maritime sector and 183 in the aviation sector.[79] However, in case of the aviation sector at least, less than one third of those accredited issuing bodies still issue cards.[80] This was confirmed by the ANAO performance audit, which found that the majority of both ASIC and MSICs (80 per cent) were issued by a small number (20 per cent) of issuing bodies.

5.126 These issuing bodies provide the intermediary service between Auscheck and the applicant, including coordinating the application and printing and issuing the actual card.

5.127 The ANAO audit made a number of findings in relation to the issuing body process. One finding was that 35 per cent of all cards were issued by commercially based 'third party' issuing bodies that have a limited ongoing relationship to the participant.[81] As a result, some issuing bodies were not consistently meeting the schemes' mandatory standards in how an applicant's operational need for a card is established.[82] Furthermore, records maintained by issuing bodies to confirm the identity of applicants were incomplete in some cases.[83] Both of these issues create vulnerabilities in the system.

5.128 Another problem noted by the ANAO related to the databases storing information about cards and cardholders. AusCheck and the issuing bodies maintain

---

79 Mr Paul Retter, Department of Infrastructure and Transport, *Committee Hansard*, 18 February 2011, p. 37.

80 Mr Paul Retter, Department of Infrastructure and Transport, *Committee Hansard*, 18 February 2011, p. 44.

81 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 15.

82 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 18.

83 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 18.

separate databases and there is no direct and ongoing link between these databases. The ANAO discovered discrepancies in the information held in each database:

> Although AusCheck has developed a range of controls over the integrity of the information entered into its database, changes in one database do not always flow through to the other. As a consequence, the two datasets differ markedly.[84]

5.129 A third potential vulnerability related to the card making process itself. Thirty-seven per cent of all ASICs and MSICs are made by an entity other than the issuing body using specialised stamping machines and licensed technology. Most card making entities were also issuing bodies, however one card maker, that had produced approximately 35 000 cards, is not and was therefore not subject to oversight by OTS.[85]

5.130 These and other issues led the ANAO to make three major recommendations (listed previously in this chapter) which the committee strongly encourages the Australian Government to attend to as a matter of urgency.

5.131 However, these issues have also led a number of witnesses to propose that the number of issuing bodies be reduced, potentially to a single issuing body. For example, Qantas was of the view that, in an ideal world, the number of issuing bodies would be reduced to one, rather than the current situation where there are over one hundred.[86]

5.132 The Transport Workers Union voiced concern that the plethora of issuing bodies undermined the integrity of the scheme due to a focus on labour supply issues rather than security. Mr Anthony Sheldon, TWU, stated:

> It is a situation that has developed since the freeing up of the ASIC process where companies have assumed those authorities. They have sought and gained approval of the issuing authorities and subsequently have issued cards, including visitors' cards and ASICs, without the scrutiny that was once provided. The changes were made to free up the time frame for people to access cards. From our experience, it has been a further diminution of the scrutiny of both ASICs and visitors' cards. Companies are just issuing them to serve a labour issue as opposed to a security or a scrutiny issue. We think that certainly warrants some serious attention.[87]

5.133 Mr Sheldon noted that a centralised, government issuing body would improve the accountability of the system, with increased scope for improving the application

---

84 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 16.

85 ANAO, *Management of the Aviation and Maritime Security Identification Card Schemes*, Performance Audit, Audit Report No, 39 2010–11, p. 18.

86 Mr Stephen Jackson, Qantas, *Committee Hansard*, 18 February 2011, p. 30.

87 Mr Scott Connolly, TWU, *Committee Hansard*, 18 February 2010, p. 57.

process as experience required.[88] The AFPA also saw the potential for a central government issuing body, suggesting that it could mirror the passport application process.[89]

5.134 The Australian Airports Association (AAA) informed the committee that there were mixed views on the subject amongst its members. Mr John McArdle, AAA, stated that:

> There is a mixed response from our membership, as you would expect. Some of them would prefer to see not only a central background checking agency but a central issuing authority, whereas others would prefer to issue the cards themselves following the successful background check...
>
> ...I would say that, of the membership, by numbers alone that [a preference for a single issuing body] would be the predominant view. However there are a couple of our major members, Sydney Airport for example, who would prefer to be the issuing authority for Sydney Airport.[90]

5.135 Sydney Airport Corporation Limited (SACL) was not necessarily against a central issuing body, but was concerned about maintaining control of access to the airport. Mr Rodney Gilmour, SACL, explained that:

> We have no difficulty with there being a central issuing authority for that. Our concern is related to access and the provision of access to the airport and we would want to retain that responsibility. But in terms of the issuing of the ASICs, that is something that we are quite relaxed about.[91]

5.136 The Office of Transport Security noted that the government had announced an intention to reduce the number of issuing bodies in the aviation sector, stating:

> ... as part of the aviation white paper announced by the government, that the minister announced that we would be moving to a series of enhancements to the ASIC regime, including a substantive reduction in the number of those issuing bodies.[92]

5.137 The committee is of the view that the Australian Government should go further and supports the establishment of a single, centralised issuing body for both ASICs and MSICs as it will improve the integrity of the scheme and allow the application and issuing process to be improved over time as experience requires.

---

88 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 64.

89 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 28.

90 Mr John McArdle, AAA, *Committee Hansard*, 17 February 2010, p. 3.

91 Mr Rodney Gilmour, SACL, *Committee Hansard*, 18 February 2010, p. 16.

92 Mr Paul Retter, Department of Infrastructure and Transport, *Committee Hansard*, 18 February 2011, p. 35.

Recommendation 22

5.138 The committee recommends that current ASIC and MSIC issuing bodies are replaced by a single, government-run, centralised issuing body.

Senator Stephen Hutchins
Chair