Parliamentary Joint Committee on Law Enforcement

Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime

June 2011

ISBN 978-1-74229-463-6

This document was prepared by the Secretariat of the Parliamentary Joint Committee on Law Enforcement and printed by the Senate Printing Unit, Parliament House, Canberra

The Committee

Members:

Senator Steve Hutchins	ALP, NSW	**(Chair)**
Senator Brett Mason	LP, QLD	**(Deputy Chair)**
Senator Steve Fielding	FFP, VIC	
Senator Stephen Parry	LP, TAS	
Senator Helen Polley	ALP, TAS	
Ms Sharon Grierson MP	ALP, NSW	
Mr Chris Hayes MP	ALP, NSW	
Mr Michael Keenan MP	LP, WA	
Mr Russell Matheson MP	LP, NSW	
Ms Maria Vamvakinou MP	ALP, VIC	

Secretariat

Dr Jon Bell, Secretary

Mr Bill Bannear, Senior Research Officer

Ms Rosalind McMahon, Administrative Officer

Previous Secretariat staff who also contributed to the inquiry are:

Mr Tim Watling, Dr Shona Batge, Dr Jacqueline Dewar, Dr Tim Kendall, Dr Robyn Clough, Ms Nina Boughey, Ms Danielle Oldfield and Ms Victoria Robinson-Conlon

Parliament House
CANBERRA

Telephone: (02) 6277 3419
Facsimile: (02) 6277 5794
Email: le.committee@aph.gov.au
Internet: http://www.aph.gov.au/Senate/committee/le_ctte/index.htm

Table of Contents

Recommendations

Recommendation 1

2.92 The committee recommends that the scope of the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003* be widened to include serious and organised crime in addition to terrorist activity and unlawful interference.

Recommendation 2

3.29 The committee recommends that security at major airports be undertaken by a suitably trained government security force.

Recommendation 3

3.52 The committee recommends that joint maritime taskforces, mirroring the functions of the Joint Aviation Investigation Teams and Joint Aviation Intelligence Groups in the maritime sector be established in every state and the Northern Territory. These taskforces should include officers of the Australian Federal Police, state or territory police, the Australian Customs and Border Protection Service and the Australian Crime Commission.

Recommendation 4

3.56 The committee recommends the formation of a Commonwealth maritime crime taskforce that would act as a national Australian Federal Police led 'flying squad', responding to specific intelligence and also conducting randomised audits of maritime and seaport security.

Recommendation 5

3.120 The committee recommends that the Attorney-General's Department conduct a review of current information sharing arrangements between law enforcement agencies and private organisations in the aviation and maritime sectors.

Recommendation 6

4.17 The committee recommends that the *Crimes (Aviation) Act 1991* be amended so as to create a new offence of deliberately travelling under a false identity.

Recommendation 7

4.27 The committee recommends that it be made a legal requirement to provide photo identification confirming passenger identity immediately prior to boarding an aircraft.

Recommendation 8

4.44 The committee recommends that the Commonwealth Government review the technical and administrative requirements necessary to facilitate the effective sharing of information between airlines and air cargo agents and law enforcement agencies and the Australian Crime Commission Fusion Centre for the purpose of enhancing aviation security and law enforcement activities. The review should include research into technical requirements for such a scheme, the costs involved and any relevant statutory or other barrier to the sharing of such information. The findings of the review should be reported to the Australian Parliament.

Recommendation 9

4.63 The committee recommends that the Australian Government provide further resources to support an increased presence for currency and illicit drug detection canine units at Australian airports.

Recommendation 10

4.81 The committee recommends that access to port security areas prescribed under the *Maritime Transport and Offshore Facilities Security Act 2003* should require verification that the Maritime Security Identification Card belongs to the individual seeking access, either through human gate operators, verification by Closed Circuit Television or any other appropriate solution.

Recommendation 11

4.94 The committee recommends the development of a system that enables the confidential movement and examination of containers that increases the likelihood that trusted insiders involved in serious or organised crime are not alerted to law enforcement agency interest in a container.

Recommendation 12

4.109 The committee recommends that the Commonwealth government further invest in CCTV at airports and ports, with consideration of a number of ongoing improvements, including:

- **that CCTV cameras should be capable of producing footage of evidential quality;**
- **the continuing lead role of Customs in coordinating the monitoring of CCTV networks; and**
- **that CCTV networks should be complemented with automated number plate recognition, and/or facial recognition technology.**

Recommendation 13

4.119 The committee recommends that Customs be given the power to revoke a depot, warehouse or broker's license if it determines, on the strength of compelling criminal intelligence, that an individual or individuals are involved or strongly associated with significant criminal activity.

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.

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.

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.

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.**

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.

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.

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.

Recommendation 22

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

Acronyms and abbreviations list

AAA	Australian Airports Association
ACAT	Aviation Criminal Assessment Team
ACC	Australian Crime Commission
ACID	Australian Criminal Intelligence Database
AFP	Australian Federal Police
AFPA	Australian Federal Police Association
AGD	Attorney-General's Department
AIC	Australian Intelligence Community
ALEIN	Australian Law Enforcement Intelligence Network
All-in	'All-in' airport policing model
ANAO	Australian National Audit Office
AQIS	Australian Quarantine Inspection Service
ASIC	Aviation Security Identification Card
ASIO	Australian Security Intelligence Organisation
ASU	Australian Services Union
ATSA	*Aviation Transport Security Act 2004*
AUSTRAC	Australian Transaction Reports and Analysis Centre
Aviation regulations	*Aviation Transport Security Regulations 2005*
Avsec	New Zealand Aviation Security Service
Beale Audit	Federal Audit of Police Capabilities
CASA	Civil Aviation Safety Authority
CCTV	Closed Circuit Television
CEO	Chief Executive Officer

CEF	Container Examination Facility
Chicago Convention	Convention on International Civil Aviation
Commonwealth Framework	Commonwealth Organised Crime Strategic Framework
Customs	Australian Customs and Border Protection Service
Customs Act	*Customs Act 1901*
ICAO	International Civil Aviation Organisation
ICS	Integrated Cargo System
IMO	International Maritime Organisation
ISPS Code	International Ship and Port Facility Security Code
JAIG	Joint Aviation Intelligence Group
JAIT	Joint Aviation Investigation Team
Maritime regulations	*Maritime Transport and Offshore Facilities Regulations 2003*
MSIC	Maritime Security Identification Card
MTOFSA	*Maritime Transport and Offshore Facilities Security Act 2003*
MUA	Maritime Union of Australia
NSW	New South Wales
NT	Northern Territory
OCA	Organised Crime in Australia Report (various years)
OTS	Office of Transport Security
PJC-ACC	Parliamentary Joint Committee on the Australian Crime Commission
PJC-LE	Parliamentary Joint Committee on Law Enforcement
PSO	AFP Protective Services Officer
SA	South Australia
SACL	Sydney Airport Corporation Limited

SCAG	Standing Committee of Attorneys-General
Smith Review	Review of Homeland and Border Security
SOCN	Serious and organised crime networks
TISN	Trusted Information Sharing Network
TWU	Transport Workers Union
UNODC	United Nations Office on Drugs and Crime
UPM	Universal Policing Model
VIC	Visitor Identification Card
WA	Western Australia
Wheeler Review	Independent Review of Airport Security and Policing
the committee	Parliamentary Joint Committee on Law Enforcement

Chapter 1
Overview of the inquiry process

Terms of reference

1.1 On 14 September 2009, the then Parliamentary Joint Committee on the Australian Crime Commission (PJC-ACC) initiated an inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime, pursuant to the committee's duties set out in paragraph 55(1)(d) of the *Australian Crime Commission Act 2002*:

> To examine trends and changes in criminal activities, practices and methods and report to both Houses of the Parliament any change which the Committee thinks desirable to the functions, structure, powers and procedures of the ACC.

1.2 Following the 2010 federal election, the committee resolved to continue the inquiry.

1.3 On 24 November 2010, the PJC-ACC became the Parliamentary Joint Committee on Law Enforcement (PJC-LE) with the added function of oversight of the Australian Federal Police (AFP), in addition to the ACC.[1] The transitional arrangements allowed the committee to continue to conduct the inquiry.[2]

1.4 The terms of reference required the committee to examine the effectiveness of current administrative and law enforcement arrangements to protect Australia's borders from serious and organised criminal activity. In particular the committee examined:

(a) the methods used by serious and organised criminal groups to infiltrate Australia's airports and ports, and the extent of infiltration;

(b) the range of criminal activity currently occurring at Australia's airports and ports, including but not limited to:

- the importation of illicit drugs, firearms, and prohibited items;
- tariff avoidance;
- people trafficking and people smuggling;
- money laundering; and
- air cargo and maritime cargo theft;

(c) the effectiveness of the Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) schemes; including the process of issuing ASICs and MSICs, the monitoring of cards issued

1 *Parliamentary Joint Committee on Law Enforcement Act 2010*, paras. 7(1)(d)–(g).

2 *National Security Legislation Amendment Bill 2010*, para. 7(1)(b).

and the storage of, and sharing of, ASIC and MSIC information between appropriate law enforcement agencies;

(d) the current administrative and law enforcement arrangements and information and intelligence sharing measures to manage the risk of serious and organised criminal activity at Australia's airports and ports; and

(e) the findings of the Australian Crime Commission's special intelligence operations into Crime in the Transport Sector and Illegal Maritime Importation and Movement Methodologies.

Conduct of the inquiry

1.5 The committee advertised the inquiry in *The Australian* newspaper and on the committee's website. In addition, the committee wrote to a range of organisations and individuals inviting submissions.

1.6 The committee received 29 submissions, of which five were confidential. The 24 public submissions were published on the committee's website. A list of submissions is included at Appendix 1.

1.7 In addition, the committee held five public hearings in Canberra, Melbourne, Sydney and Perth. The witnesses who appeared before the committee at these hearings are listed at Appendix 2.

1.8 The committee also conducted a number of site visits to airports, seaports and other facilities around Australia. A list of places visited is included at Appendix 3.

Terminology

1.9 It should be noted that some international jurisdictions employ the term 'serious organised crime' whereas the convention in Australia is to use the term 'serious and organised crime'. These terms are used interchangeably within this report. In some cases the abbreviated 'organised crime' is also used.

1.10 Other abbreviations and acronyms are listed in the glossary.

Structure of report

1.11 The chapters of this report are organised around the key themes which emerged during this inquiry and therefore do not directly mirror the terms of reference.

1.12 Chapter 2 provides an overview of the major themes of the inquiry. This includes the background to the inquiry and an analysis of the threat of serious and organised crime in the aviation and maritime sector. It concludes with a number of issues that informed the committee's recommended course of action.

1.13 Chapter 3 deals with the issues of intelligence sharing and agency cooperation and coordination. This includes the security and policing models in place at airports and ports and the use of key intelligence in order to inform the law enforcement response.

1.14 Chapter 4 focuses on security measures within the aviation and maritime sectors which minimise vulnerabilities that can be exploited by serious and organised criminal networks. Referred to as 'target hardening', such measures focus on improving the physical environment and vulnerable processes within that environment.

1.15 Chapter 5 addresses the ASIC and MSIC schemes. A number of current vulnerabilities are noted along with relevant recommendations.

Acknowledgements

1.16 The committee wishes to express its appreciation to all parties that contributed to the conduct of this inquiry, whether by making a written submission or through attendance at a hearing, or in many cases, both.

1.17 As part of this inquiry the committee conducted a number of site visits, which enabled it to gain a more in-depth understanding of the issues and agencies involved in combating serious and organised crime in Australia. Accordingly, the committee would like to thank officers from the Australian Customs and Border Protection Service, the ACC, the AFP and state and territory police. In addition, the committee would like to thank the many private organisations that assisted the committee in accessing airport and port facilities.

1.18 The committee would also like to acknowledge the assistance and expertise provided by those state and territory Commissioners of Police and senior police officers who met with the committee during this inquiry.

Chapter 2

Evaluating and responding to the threat

Introduction

2.1 Over the course of this inquiry, the committee has received significant evidence of infiltration of the aviation and maritime sectors by serious and organised criminal networks (SOCN). This is a natural consequence of the strong incentives that exist within those sectors for profit-seeking organised criminals.

2.2 The law enforcement response to this threat has become increasingly coordinated through a variety of mechanisms discussed in this report. As always, the response, including government policy, will need to adjust to an evolving threat.

2.3 In this chapter, the committee provides an overview of the threat posed by serious and organised crime in the aviation and maritime sectors, as well as the national response. In addition, the committee presents a number of observations that serve as principles to underpin an effective government response.

The threat of serious and organised crime in the aviation and maritime sectors

2.4 Evidence provided to the committee by the Australian Crime Commission (ACC) and other law enforcement agencies and obtained during an extensive set of site visits around the country have led the committee to the view that serious and organised criminality in the aviation and maritime sectors poses a very real threat to Australia.

2.5 It is also important to note that while serious and organised criminal activity is taking place across Australian airports, seaports and beyond, the majority of individuals working within those environments are law-abiding employees engaged in legitimate activity. Nevertheless, a small minority of individuals within those sectors have been found to be involved in serious criminal activity (as has been the case in other sectors). Transportation networks are a valuable target for organised crime, given the potential use of those networks to facilitate lucrative illicit operations. Given the importance of transport sectors to facilitating both licit and illicit economic activity, that small minority of individuals can have a relatively high impact.

2.6 The following section outlines a selection of public evidence relating to the threat of serious and organised crime in the aviation and maritime sectors. Additionally, the committee has received evidence in-camera and in private discussions that further support these claims. However, the committee is of the view that the publication of such evidence would be against the public interest and has not included confidential evidence in this report.

The evolving nature of organised criminal networks

2.7 As noted in the Commonwealth Organised Crime Strategic Framework, criminal networks are driven by a profit motive, which generally differentiates them from politically motivated terrorist networks. Organised criminal networks are driven by a desire to make, and subsequently hide, illicit profits. Demand for illicit commodities, such as drugs, is likely to remain strong, driving the criminal economy by providing a strong profit incentive to engage in organised criminal activities. Organised criminal networks seek to balance profit opportunities with attendant risks of detection and prosecution. [1]

2.8 Increasingly, SOCNs operate across borders. Facilitated by advances in communication and travel, organised crime has become a globalised affair, with networks of immense size involved across markets and sectors.[2] As the ACC notes in the Organised Crime in Australia 2011 Report:

> The power, networking ability and opportunism of sophisticated transnational criminal groups means they now operate at an unprecedented level around the world. Some groups wield immense power. The reach and influence of leading members of the larger transnational crime groups stretches far beyond their home country. For example, Mexican drug cartels now have a foothold on most continents and profits that rival the GDP of some of the world's smaller nations.[3]

2.9 In Australia, organised criminal activity is undertaken by a number of highly interconnected groups and individuals, working together in loose networks on an opportunistic basis.[4] The public perception of stereotypical organised crime groups is increasingly inaccurate. While outlaw motorcycle gangs, underworld figures and hierarchical and highly-controlled organised crime groups remain significant, there has been increasing cooperation between traditionally rival groups as opportunities arise.[5]

2.10 These loose networks are extremely flexible. The ACC notes that current patterns of organised crime are more complex than at any other time in history.[6] They are sensitive to the tactics employed by law enforcement and regulatory agencies and are able adjust their operations in response.[7] In part, the need for this flexibility has been behind a shift away from traditional, hierarchical organised crime models, as explained by the ACC:

---

1 Australian Government, Commonwealth Organised Crime Strategic Framework, p. 9.

2 Australian Crime Commission, Organised Crime in Australia 2011 Report, March 2011, p. 3.

3 ACC, OCA 2011, pp 24–25.

4 ACC, OCA 2011, p. 25.

5 Commonwealth Framework, p. 8.

6 ACC, OCA 2011, p. 3.

7 ACC, OCA 2011, p. 3.

> Internationally, traditional hierarchies, typified by the Sicilian Mafia or the Yakuza in Japan, remain resilient and effective in their specific markets. However, other transnational criminal enterprises have varied traditional hierarchical command and control structures by moving to adaptable and more flexible structures, including in some cases franchise models.
>
> Traditional hierarchical organised criminal groups are increasingly responding to changing market dynamics and law enforcement interdiction. They are offsetting the disadvantages inherent in rigid and sometimes brittle hierarchical command structures through networked or hybrid structures and innovative use of information and communications technologies.[8]

2.11 SOCNs infiltrate various sectors of the economy in order to facilitate illicit activity and profits. As a result, criminal activity is supported, knowingly or otherwise, by a range of people with access to information, infrastructure, government services, knowledge of institutional weaknesses or access to specialist skills.[9] The importance of these 'facilitators' or 'trusted insiders' is discussed below.

2.12 As a result of infiltration, networks have established a significant foothold in certain industry sectors. As noted in the Commonwealth Framework, once these footholds are established, organised crime can more easily profit from these sectors and become resistant to law enforcement interventions.[10]

2.13 SOCNs are knowledgeable of legitimate industry practices, demonstrating a high degree of resilience to traditional organised crime interventions. [11] They are able to operate within and alongside legitimate businesses and may work across industries in order to maximise return and minimise risk, in much the same way a legitimate business would.[12]

2.14 SOCNs can be expected to actively exploit current and emerging opportunities to generate funds or otherwise benefit from a broad range of activities of interest to the Commonwealth.[13] The importance of the aviation and maritime sectors in facilitating a number of lucrative criminal activities suggests that they are a prime target for infiltration.

2.15 The majority of serious and organised criminal activity in Australia is focused on illicit drug markets, although other activities include tax evasion, money laundering, fraud, identity crime and high tech crime.[14]

---

8 ACC OCA 2011, p. 26.

9 Commonwealth Framework, p. 9.

10 Commonwealth Framework, p. 9.

11 Commonwealth Framework, p. 8.

12 ACC, OCA 2011, p. 3.

13 Commonwealth Framework, p. 9.

14 ACC OCA 2011, p. 4.

2.16 The impact of organised crime in Australia is serious and far exceeds the direct harm caused by the specific offences. As the ACC explains in the 2011 Organised Crime in Australia Report:

> In fact, the activities of high threat serious and organised criminal enterprises result in significant harm to the Australian community. There are significant losses to the economy, including the redirection of resources that might otherwise be invested in legitimate business, reductions in tax revenue and increasing costs of law enforcement and regulation. The widespread impact extends to costs associated with longer-term health and social harm. The activities of organised criminal enterprises can also undermine public confidence in the integrity of key business sectors and government institutions.[15]

2.17 The ACC conservatively estimates the direct cost of serious and organised crime in Australia to be between $10 and 15 billion every year. In addition, indirect costs such as those associated with illicit drug addiction, forced prostitution and community violence are also significant. Illicit drug abuse alone has an estimated social cost of over $8 billion annually. There are also other serious impacts including the collateral damage to family relationships, community functions and social cohesion, and potentially the loss of public confidence in the rule of law and the administration of justice.[16]

The Australian Crime Commission special intelligence operations

2.18 The terms of reference to this inquiry require it to examine the findings of the ACC's special intelligence operations into crime in the transport sector and iIllegal maritime importation and movement methodologies.

2.19 The *Crime in the Transport Sector Determination* was operational from November 2005 to June 2008, producing some 395 reports related to the maritime sector, including three strategic intelligence reports and five policy discussion papers. An additional 91 reports related to the aviation sector.[17]

2.20 The *Illegal Maritime Importation and Movement Methodologies Determination* was operational between November 2006 and December 2008 and produced 177 reports, including six strategic intelligence reports and three policy discussion papers on small craft and domestic fishing environments.[18]

2.21 In addition to those two determinations, the ACC's Aviation Criminal Assessment Team (ACAT) was established following a recommendation of the

---

15 ACC OCA 2011, p. 4.

16 ACC OCA 2011, p. 4.

17 Mrs Karen Harfield, Acting Chief Executive Officer, ACC, *Committee Hansard*, 17 February 2011, pp 7–8.

18 Mrs Karen Harfield, Acting CEO, ACC, *Committee Hansard*, 17 February 2011, pp 7–8.

Independent Review of Airport Security and Policing for the Government of Australia, conducted by the Rt Hon Sir John Wheeler in 2005 (the Wheeler Review).[19] Since then ACAT has produced and disseminated 69 intelligence products specific to the aviation environment.[20]

2.22 Through its special intelligence operations, the ACC found evidence of infiltration of the airport and port environments by serious and organised crime. The majority of identified organised criminality involved the larger metropolitan container ports and international airports, although criminal activity at smaller and regional ports and in general aviation was also observed. 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 those environments, criminal groups have exploited gaps, weaknesses and inconsistencies in the application of the regimes.[21]

The nature of organised crime in the aviation and maritime sectors

2.23 The aviation and maritime sectors are highly desirable targets for serious and organised criminal networks. They are the key link to the international illicit economy, facilitating the importation of illicit goods (particularly drugs) and a range of other crimes detailed below.[22] As a result, criminal networks have an incentive to infiltrate these sectors in order to engage in a number of highly profitable criminal activities.

2.24 As noted above, as serious and organised crime infiltrates various sectors of the economy, its activities are often supported (knowingly or otherwise) by a range of people with access to information, infrastructure, government services, knowledge of institutional weaknesses or access to specialist skills.[23] These individuals or groups are referred to as facilitators or trusted insiders.

Facilitators

2.25 As noted in the Commonwealth Framework, facilitators with specific skill sets play a vital role, sometimes unintentionally, in assisting criminal networks to operate undetected and seamlessly across both legitimate and illicit markets.[24] Internal

19 The Rt Hon Sir John Wheeler, Australian Government, 'An Independent Review of Airport Security and Policing for the Government of Australia', September 2005; see Recommendation III.

20 Mrs Karen Harfield, Acting CEO, ACC, *Committee Hansard*, 17 February 2011, pp 7–8.

21 Mrs Karen Harfield, Acting CEO, ACC, *Committee Hansard*, 17 February 2011, p. 8.

22 ACC, *Submission 8*, p. 4.

23 Commonwealth Framework, p. 9.

24 Commonwealth Framework, p. 9.

facilitators collude to facilitate the exploitation of vulnerabilities within the sector and often commit criminal offences themselves.[25]

Trusted insiders

2.26 The term 'trusted insider' refers to individuals working within a sector, who are able to act on behalf of criminal networks. These insiders occupy positions of trust, in that they have obtained the necessary security clearances to maintain access to sensitive areas. They are trusted by external criminal groups to conduct criminal activity but are rarely themselves the principal involved in criminal acts.[26] Trusted insiders will generally have no criminal record and may have worked in trusted positions within the sector for some time.

2.27 Trusted insiders and facilitators assist organised crime groups through enabling activities such as:

- deliberately ignoring criminality;
- influencing human resource processes to facilitate possible criminal activity;
- providing information or advice to criminal groups about vulnerabilities within the sector;
- allowing criminal associates access to uncleared goods; and
- actively participating in the commission of an offence.[27]

Features of crime in the maritime and aviation sectors

2.28 The submission by the ACC to the committee's inquiry outlines the methods used by organised crime groups in conducting criminal activity using Australia's ports and airports. Most of the methods listed below require the use of facilitators or trusted insiders within the industry.

2.29 The focus of criminal activity is on the importation of illicit goods, with drugs being the most common commodity. However, the range of criminal activity also includes money laundering, firearms movement, smuggling of flora and fauna, theft, tariff and excise evasion and counterfeiting.[28]

Maritime sector

2.30 Generally, the maritime sector has been more important to organised crime groups than aviation, mostly due to the greater volume of traded goods passing through ports. Methods used by criminal networks include:

---

25 ACC, *Submission 8*, p. 6.

26 ACC, *Submission 8*, p. 6.

27 ACC, *Submission 8*, p. 9.

28 ACC, *Submission 8*, p. 11.

- rip on/rip off—this method involves internal facilitators at the originating or transit port placing bags of illicit items into already packed shipping containers for retrieval before customs inspection. Neither the consignor or the consignee is aware that an illicit commodity has been transported within their consignment;
- piggybacking—this involves the criminal importing syndicate using the identity and credentials of an unsuspecting legitimate importer to clear the shipment through customs without the knowledge of the listed consignee, thereby 'riding on the back' of the legitimate consignee's reputation;
- nominal consignee—in this methodology the 'nominal' consignee is aware the shipment is coming as the shipping documentation lists the 'nominal consignee' as the importer of the listed goods. However, they are only the interim consignee because they are concealing the identity of the true importer;
- theft of containers—there have been cases where whole containers full of goods have been stolen from Australian ports and depots. While the majority of container theft is related to tobacco or other high value/high duty goods, this methodology may also facilitate a major importation of illicit commodities to Australia.[29]

2.31 These methods are significantly assisted by criminally complicit maritime workers acting as trusted insiders or facilitators within the Australian maritime sector.[30]

2.32 ACC intelligence has identified persons linked to nationally significant serious and organised crime groups as present within the maritime environment. This includes members, associates or affiliates of ethnically based organised crime groups, significant regional crime syndicates or persons and outlaw motorcycle gangs.[31]

2.33 Criminality within the port environment is spread across the various work and skill types, and involves a range of industry groups within or linked to the maritime sector.[32]

2.34 The ACC has assessed that there are higher levels of criminality present in New South Wales and Victorian container ports. It noted that this observation reflects vulnerabilities presented by the volume of cargo, workforce size, the local criminal environment and the proximity of these ports to the major illicit commodity markets.[33]

---

29 ACC, *Submission 8*, p. 5.

30 ACC, *Submission 8*, p. 6.

31 ACC, *Submission 8*, p. 7.

32 ACC, *Submission 8*, p. 7.

33 ACC, *Submission 8*, p. 7.

2.35 The Australian Customs and Border Protection Service (Customs) agreed with this assessment, noting the different risk profile associated with major and minor ports. As Mr Jeff Buckpitt, Customs, noted:

> Sydney and Melbourne are the key ports of highest risk in terms of drugs entering by sea cargo. All ports are a risk, but historically if you look at where the detections have occurred the vast majority of them has been in Sydney followed then by the ports of Melbourne and Brisbane.[34]

2.36 The committee was able to visit a range of port facilities during the inquiry and observed that security arrangements varied depending on the size and profile of the port.

Small boat importation

2.37 Another method used by organised criminal networks in the importation of illicit substances is the use of small craft and fishing vessels.[35] This method has received exposure recently, with the seizure of 464 kilograms of cocaine from a yacht in Brisbane.[36]

2.38 The ACC described a number of criminal methodologies involving small craft, including the burying of illicit consignments at sea, meeting at sea or commercial drop offs, direct arrival by small craft, aerial drop offs and the use of semi-submersibles.[37]

2.39 The committee was informed that there has been a lack of detected small craft illicit drug importations into Australia, which is not consistent with global trends. It is likely that these activities are ongoing, as evidenced by the case above.[38]

Aviation sector

2.40 The aviation sector is also vulnerable to the type of infiltration described above. Facilitators or trusted insiders, either placed by criminal networks or recruited from the aviation workforce, assist the networks by ignoring criminality, recruiting associates, providing sensitive information about the sector's vulnerabilities and law enforcement arrangements or by actively participating in the commission of an offence.[39]

---

34 Mr Jeff Buckpitt, Australian Customs and Border Protection Service, *Committee Hansard*, 17 February 2011, p. 5.

35 ACC, *Submission 8*, p. 7.

36 ABC News, '$160m cocaine bust on Brisbane yacht', 14 October 2010, http://www.abc.net.au/news/stories/2010/10/14/3037967.htm (accessed 21 April 2011).

37 ACC, *Submission 8*, p. 8.

38 ACC, *Submission 8*, p. 8.

39 ACC, *Submission 8*, p. 9.

2.41 The ACC notes that there are criminal groups operating wholly within the aviation sector, with a focus on air cargo. These groups tend to commit ongoing offences such as tariff avoidance, excise fraud, theft of air freight, and narcotic distribution and importation. The international aviation sector has also been used to facilitate money laundering.[40]

> Some of the more serious incidents of criminal infiltration of the sector involve specific occupational groups with positions providing access to airports or in some cases in associated external premises such as bond stores. Activities by these entities have included fraud in relation to duty free goods, money laundering, domestic drug supply and trafficking and narcotic importations. Many of these positions involve access to airside security areas or where individuals acting alone retain the capability to facilitate criminal activity.[41]

2.42 Outside of the major airports, there are approximately 2000 operational airports and airstrips with most having little to no screening. This provides an alternate method for those seeking to circumvent security screening processes.[42]

The price of illicit drugs: a strong incentive

2.43 Given that the importation and distribution of illicit drugs is the main type of serious and organised criminal activity undertaken in the aviation and maritime environment, the committee sought more detail on the degree of profit involved. Data provided by the ACC, including international data compiled by the United Nations Office on Drugs and Crime indicates the extreme difference between Australian and international drug prices (see Appendix 4). This difference is likely to make Australia an extremely lucrative target for drug smuggling syndicates.

2.44 For example, the wholesale price for a kilogram of cocaine in Colombia, a source country, is reported to be US$2348.[43] By comparison, the same amount of cocaine had an Australian wholesale price (in United States Dollars) of between $150 000 to $250 000.[44] The retail prices could range between $300 000 and $1 million for a kilogram cut into 'street deal' packages. By comparison, wholesale prices in the United States, United Kingdom and Canada ranged between $10 000 to approximately $70 000 per kilogram.

2.45 As Mr Michael Phelan, Deputy Commissioner, Australian Federal Police (AFP), explained, drug prices respond to the same market forces affecting every other commodity:

---

40 ACC, *Submission 8*, p. 10.

41 ACC, *Submission 8*, p. 10.

42 ACC, *Submission 8*, p. 10.

43 ACC, International and Domestic Drug Prices, *Tabled Document*, 17 February 2011.

44 ACC, International and Domestic Drug Prices, *Tabled Document*, 17 February 2011.

> Drugs in particular [are] just like every other commodity in the world: whether we are talking about copper or gold, the price is driven by the standard economic equation of supply and demand. Demand in Australia is high. The price is not the driver; it is demand, which is high. For cocaine, for example, the reason the price is a lot lower in the United States is because supply is a lot easier in the United States than it is here. Those that are willing to pay for it at that particular price slide you up the demand curve and the price curve and you end up paying those terrible wholesale prices for it, which in turn see the profits and people willing to do it. It is a couple of years salary, the wholesale price for a kilo of cocaine.[45]

2.46 Mrs Karen Harfield, ACC, informed the committee that the high Australian price for drugs was likely to affect the decision-making of international criminal networks:

> On the basis of our assessment, a well-described motive for serious and organised crime is profit. The reality is that they will attempt to infiltrate the markets that give them the biggest profit margin. Obviously drugs are available across the globe, so we are not the only target but the price will have some affect on the decision making.[46]

2.47 The committee acknowledges that the high prices of illicit drugs, no doubt driven by the high demand for such commodities by Australian citizens, means organised criminal networks are likely to go to great lengths to circumvent security measures designed to combat importation of such substances.

Other crime

2.48 The committee also received evidence regarding a number of other types of crime, most notably including tobacco smuggling and money laundering.

Tobacco smuggling

2.49 Mr Richard Janeczko informed the committee that organised, and some not so organised, criminal networks were targeting the importation of undeclared tobacco, seeking to profit from the high duties imposed on that product. As Mr Janeczko explained:

> I believe that organised crime chases the money and I made a number of statements while I was still working in Customs and I have repeated them since that because of the huge amount of profits involved it attracts organised criminals. I was asked a number of times in public about whether there was a relationship between duty rates and tobacco smuggling and I said there was. If you walk along a footpath and found five cents, you might not pick it up but if it was a $100 note, you would definitely pick it up. I

45 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 45.

46 Mrs Karen Harfield, Acting CEO, ACC, *Committee Hansard*, 17 February 2011, p. 10.

> think smuggling is a bit like that. You mentioned drugs earlier. I think there is a huge level of organised crime involved in bringing tobacco into Australia.[47]

2.50 Mr Janeczko explained that the tobacco was sourced from a number of countries, observing:

> China is a major manufacturer. Indonesia and the Philippines are also manufacturers. A lot of the tobacco, though, that comes into Australia is routed through other ports. But China is a huge source of tobacco that is smuggled in, as is Indonesia.[48]

2.51 Mr Janeczko elaborated that the illegal tobacco that is currently being seized and prosecuted by Customs ranges from a leaf that has been chopped up to counterfeit product and to legally imported tobacco that is redirected.[49]

Money laundering

2.52 Money laundering is an essential activity for serious and organised criminal networks. Illicit profits require a mechanism by which the money can eventually be used in the legitimate economy. As a result, legitimising the proceeds of crime is a crucial process for organised criminal networks.[50]

2.53 The committee is aware that both aviation and maritime transport routes are used in the remittance of illicit profits both internationally and domestically. For example, the ACC submission to the inquiry includes a case study of money laundering using flight crew on international routes.[51]

Committee view

2.54 After nearly two years of inquiry, the committee is of the opinion that serious and organised crime occurs within the aviation and maritime sectors, and that the level of activity demands a strengthened response by the Australian and state governments, working together with sector stakeholders. The current response is described in the next section.

---

47 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 14.

48 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 15.

49 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 15

50 ACC, OCA 2011, p. 46.

51 ACC, *Submission 8*, p. 10.

Responding to the threat

Law enforcement approach

2.55 Law enforcement agencies continue to undertake the lead role in responding to the threat of organised crime. That response is not limited to certain areas, such as the aviation and maritime sectors, but necessarily adopts a comprehensive approach. As the evidence above suggests, organised criminal networks have footholds in many areas and only a combined whole-of-government response will be effective.

2.56 The law enforcement response to organised crime is therefore becoming increasingly sophisticated. Recent improvements include:

- the recognition of serious and organised crime as a threat to national security requiring the attention of both law enforcement and national security agencies;
- the creation of a Commonwealth Organised Crime Strategic Framework to coordinate the approach taken by various law enforcement agencies; and
- the establishment of the Criminal Intelligence Fusion Centre to allow faster and more accurate exchange of criminal intelligence between agencies.

2.57 The committee has found that the law enforcement approach within the aviation and maritime sectors could be improved in a number of specific ways. The majority of these findings appear in Chapter 3, which deals with information sharing and agency coordination. However, it is important to recognise that fighting organised crime in the aviation and maritime sectors cannot occur in isolation, but must fit within the national (and international) strategy.

Regulation of the sector: development of domestic transport security policy

2.58 Current aviation and maritime transport security policy within Australia has been developed in order to prevent a terrorist attack on aviation and maritime infrastructure. Following 11 September 2001, there has been an increasing international focus on the need for a system to secure the aviation and maritime transport sectors against the threat of terrorism.

2.59 Maritime security policy has been guided by the International Ship and Port Facility Security (ISPS) Code, developed by the International Maritime Organization (IMO) in December 2002.[52]

2.60 The Australian Government developed the *Maritime Transport Security Act 2003* to implement the ISPS Code in Australia. Both the ISPS Code and the Act came into effect on 1 July 2004. In 2005 the Act was extended to cover offshore oil and gas

52 Department of Infrastructure and Transport, *Submission 18*, p. 3.

facilities and renamed the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA).[53]

2.61 Aviation security policy has been informed by the 'Chicago' Convention on International Civil Aviation, to which Australia is a signatory, which is overseen by the International Civil Aviation Organisation (ICAO). The relevant annex to the convention sets out requirements pertaining to the safeguarding of passengers, crew, ground personnel and the general public in matters related to unlawful interference with civil aviation; establishing an organisation to develop and implement appropriate domestic regulations, practices and procedures; and ensuring that the principles applied to international civil aviation are applied to domestic aviation to the extent practicable.[54]

2.62 The Chicago Convention requirements were given domestic force through the *Aviation Transport Security Act 2004* (ATSA), backed by the Aviation Transport Security Regulations 2005. These establish the legal framework for a security regime under which aviation industry participants themselves are required to act to reduce security risks to their operations. The stated purpose of the ATSA is to establish a regulatory framework to safeguard against unlawful interference with aviation transport.[55]

2.63 The administration of both ATSA and MTOFSA was enhanced in December 2004 through the creation of the Office of Transport Security (OTS), a business division of what is now the Department of Infrastructure and Transport.[56] OTS was established as the primary advisor to the Australian Government on transport security policy. As the transport security regulator, OTS is responsible for bringing security responsibilities for the aviation and maritime sectors together in a single national regulatory approach.[57]

2.64 Key measures included in ATSA and the associated regulations, include:

- a requirement for industry participants to develop and comply with a transport security plan that sets out security measures and procedures based on a security risk assessment of their operation;
- the designation of secure areas (broadly divided into airside and landside zones, include 'sterile' landside zones) within all major metropolitan airports, larger metropolitan General Aviation airports and many regional airports;

---

53 Department of Infrastructure and Transport, 'Maritime Security', http://www.infrastructure.gov.au/transport/security/maritime/index.aspx (accessed 21 April 2011).

54 Wheeler Review, p. 12.

55 Department of Infrastructure and Transport, *Submission 18*, p. 4.

56 Department of Infrastructure and Transport, *Submission 18*, p. 3.

57 Department of Infrastructure and Transport, *Submission 18*, pp 3–4.

- screening of people, goods and vehicles, to remove the likelihood of weapons and prohibited items being taken into secure areas or onboard aircraft;
- regulation of the air cargo sector, through the accreditation of Regulated Air Cargo Agents; and
- the provision of certain powers and exemptions to suitably trained screening officers, airport security guards, law enforcement officers, and aviation security inspectors.[58]

2.65 These mirror broadly similar measures provided through MTOFSA and its associated regulations, including:

- The establishment of three security levels of increasing risk, including appropriate security settings for each given security level;
- a requirement for industry participants to develop and comply with a maritime security plan that sets out security measures and procedures based on a security risk assessment of their operation;
- the establishment of maritime security zones (including land-side restricted zones, cleared zones and water-side restricted zones) to protect critical areas within security regulated ports, and on or around ships (in port or at sea) or offshore facilities;
- screening of people, goods and vehicles entering a 'cleared zone' to prevent anyone taking weapons and prohibited items on board passenger ships; and
- the provision of certain powers and responsibilities to suitably trained screening officers, maritime security guards, law enforcement officers, duly authorised officers and maritime security inspectors.

2.66 These measures are complemented by the Aviation Security Identity Card (ASIC) and Maritime Security Identity Card (MSIC) schemes, which seek to ensure that individuals employed in or regularly accessing secure areas in the aviation and maritime sector are subject to a certain level of background checking.

2.67 The ASIC scheme was introduced in 1998 but has been subject to a number of changes in subsequent years. Originally, applicants were subject to a criminal record check only. However, following the September 11 terrorist attacks, the scheme was expanded to cover a greater number of airports and strengthened through the introduction of tighter criminal history checks and an Australian Security Intelligence Organisation (ASIO) security assessment.[59]

2.68 The MSIC scheme was introduced in 2005, with full implementation in 2007, and was the first of its kind in the world to check the background of all people who have unmonitored access to sensitive areas of ports, port facilities, ships and offshore

58 Department of Infrastructure and Transport, *Submission 18*, pp 4–8.

59 Department of Infrastructure and Transport, *Submission 18*, p. 9.

facilities.[60] As with the ASIC scheme, applicants are subject to a criminal history check and an ASIO security assessment. Additionally, applicants for either an ASIC or an MSIC may be subject to an unlawful non-citizen check conducted by the Department of Immigration and Citizenship.[61] The ASIC and MSIC schemes are discussed in detail in Chapter 5.

Extending aviation and maritime security measures to cover serious and organised crime

2.69 As described above, the aviation and maritime security regimes, as enacted through ATSA and MTOFSA, have focused on reducing the risk of a terrorist attacks on aviation and maritime infrastructure. Mr Paul Retter, Department of Infrastructure and Transport, elaborated on the intent of the acts, stating:

> Their purpose is primarily to ensure a more secure transport system for Australia. They are essentially focused on unlawful interference with vessels and aircraft and the range of activities that come under the definition of unlawful interference—taking control of an aircraft or vessel by force or threat of force or other forms of intimidation or trick or false pretence, destroying an aircraft or a vessel, causing damage to an aircraft or vessel that is in service and so on and so forth.

2.70 Mr Retter went on to explain that serious and organised crime was not currently included in the scope of the legislation, stating:

> ...the purpose of those two acts, when they were placed on the statutes and implemented, was primarily to deal with a terrorism threat, not a serious and organised crime issue. Our focus and the focus of the act and the associated regulations, including the various layers of security that we have in place as a preventive security regime in the aviation and maritime sectors, is about preventing unlawful interference in the context of terrorism. The issue that you raise, quite frankly, is an issue that I know has been debated—the policy position on whether or not the purpose of the acts should be changed.[62]

2.71 The committee has formed the view that the purpose of the act does need to expand to include the threat of serious and organised crime, for reasons outlined below.

2.72 Two recent high level reviews have spoken of the need to expand the Australian Government's national security focus to include the threat posed by serious and organised crime.

---

60 Department of Infrastructure and Transport, *Submission 18*, p. 18.

61 Department of Infrastructure and Transport, *Submission 18*, pp 18–19.

62 Mr Paul Retter, Office of Transport Security, *Committee Hansard*, 18 February 2011, p. 40

2.73 In June 2005, the Australian Government invited the Rt Hon Sir John Wheeler to conduct a review into airport security and policing (the Wheeler Review). The report made a number of recommendations, particularly relating to information sharing, agency cooperation and airport policing models, which have informed the analysis in subsequent chapters. The review also made the point that the threat of terrorism and crime were not necessarily separate issues, stating:

> Terrorism and crime are distinct, but potentially overlap. At its most basic, a culture of lax security or petty criminality can provide opportunities for terrorists to exploit weaknesses in airport security. Staff can be bribed to ignore criminality or paid large sums to assist in drug trafficking or theft. Once compromised, such employees may be unable to stand up to terrorists. Any airport staff who are not thoroughly background checked and routinely searched are potential weak links.[63]

2.74 The Wheeler Review argued that the terrorism, organised crime and opportunistic crime constitute the major security threats to Australia's airports.[64] Several recommendations in the report relating to airport policing models were adopted by the government and are discussed in more detail in Chapter 3.

2.75 In 2008, Mr Ric Smith, a former Secretary of Defence, was invited to conduct a review of homeland and border security (the Smith Review). Though the report was confidential, a summary document was publicly released. The summary report called for a greater coordination of agencies and departments in the national security field, including an enhanced leadership position in the form of a National Security Adviser, which was duly established in December 2008.[65]

2.76 In addition, the report also argued that while the national security agenda had emphasised counterterrorism arrangements in the post-September 11 environment, it was time to provide an additional focus on other threats and hazards, including emergency management, serious and organised crime and electronic attack.[66] On serious and organised crime in particular, the report summary stated:

> Serious and organised crime, as an ever present threat to the safety and prosperity of Australians and a challenge to the integrity of our institutions, is as important as any other security threat, with an estimated cost in excess of $10 billion per year. Crime is increasingly sophisticated and transnational. The states and territories have major roles and the Commonwealth needs to engage effectively with them in this area. The current arrangements for coordinating Commonwealth efforts and priorities are limited. There are some gaps in national efforts, such as limited sharing

63 Wheeler Review, p. ix.

64 Wheeler Review, p. 7.

65 The Hon. Kevin Rudd MP, 'The First National Security Statement to the Parliament', Speech, 4 December 2008, http://pmrudd.archive.dpmc.gov.au/node/5424 (accessed 8 April 2011).

66 Mr Ric Smith AO PSM, Report of the Review of Homeland and Border Security, Summary and Conclusions, p. 4

> of police capabilities and case management databases, and more attention could be given to criminal intelligence collection and analysis. A strategic framework for Commonwealth efforts in relation to serious and organised crime should be developed for consideration by government.[67]

2.77 Following on from the Smith Review and the then Prime Minister's inaugural National Security Statement to the Parliament, the Commonwealth Organised Crime Strategic Framework was established in November 2009.[68] The framework features three key elements, which are:

- an Organised Crime Threat Assessment to provide a shared picture among relevant stakeholders of the most significant threats and harms arising from organised criminal activity;
- an Organised Crime Response Plan to align Commonwealth efforts to both identified and emerging organised crime threats; and
- multi-agency responses to develop and deliver operational, policy, regulatory and legislative responses to organised crime.

2.78 The objectives of the framework are directly applicable to the committee's recommendations in Chapter 3, which deal with information sharing and agency collaboration.

2.79 Serious and organised crime cannot be divorced from national security considerations. The ACC notes that maritime and aviation security presents significant national security issues.[69] In its submission to the inquiry, the ACC stated:

> The nexus between terrorism and criminality suggests that safeguarding the maritime port and aviation environments against terrorist attack, and the detection and prevention of sector based crime are closely interrelated objectives. Hence, the disruption of crime within the maritime and aviation sectors and the prevention of terrorism are not, and should not be considered, mutually exclusive objectives.[70]

2.80 While terrorist and criminal organisations have differing and often conflicting motives, the methodologies developed by organised criminal networks can also be used to facilitate acts of terror. Mrs Karen Harfield, ACC, remarked upon the importance of tackling terrorism and serious and organised crime, stating:

> Both terrorist groups and criminal groups have consistently been noted as primary threats to Australia's transport sector. The Wheeler review noted that terrorism, organised crime and opportunistic crime present the three

---

67 Mr Ric Smith AO PSM, Report of the Review of Homeland and Border Security, Summary and Conclusions, p. 4

68 The Hon Robert McClelland MP and the Hon Brendan O'Connor MP, 'Organised Crime Strategic Framework', Joint Media Release, 25 November 2009.

69 ACC, *Submission 8*, p. 5.

70 ACC, *Submission 8*, p. 5.

> primary threats to aviation and airports. Recognition of the threat presented by terrorism also generated enhancements to the maritime environment security regime implemented under the maritime environment security regime implemented under the Maritime Transport and Offshore Facilities Security Act 2003.
>
> Likewise, the Department of Infrastructure and Transport, in their 2009 Aviation Security Risk Context Statement, reported that criminal activity can expose aviation security vulnerabilities that might be exploited by terrorists. More recently, the foiled Yemeni bomb plots illustrate that terrorist organisations are mimicking drug importation methodologies that have been utilised by criminal groups for some time. Disruption of crime within the aviation and maritime sectors and the prevention of terrorism need not be considered mutually exclusive objectives.[71]

2.81 Detective Superintendent Charlie Carver, WA Police, was also of the view that terrorism and organised crime were increasingly linked, stating:

> Principally, the actual driver of organised crime is wealth. However, there have been links to terrorism in the past. You only have to look at al-Qaeda. That was fuelled by organised crime funding through Afghanistan, through the heroin trade... You only have to look closer to our borders in relation to Indonesia. You had the Bali incidents and also at Jakarta they were using drugs and also armed robberies to fuel their activities—organised crime again. It is my view that the link between that and organised crime is closer than what a lot of people think. I know that a lot of the other things that have been put in place in relation to terrorism concentrate on terrorism, but I believe that there is a closer link even more today than there has been in relation to serious and organised crime. They are getting closer and closer every year that goes by.[72]

2.82 The ACC's 2011 Organised Crime in Australia Report noted that the increasingly globalised nature of organised crime meant that there was a growing risk of linkages with terrorist organisations occurring. As the report stated:

> The activities of transnational organised crime groups and some terrorist groups converge where their illicit networks intersect. Failed, failing and rogue states provide safe havens for organised crime, impetus for the production and distribution of illicit commodities and an environment where organised criminal activity and the interests of extremist or terrorist groups can converge...
>
> ...The convergence is of most concern when it is married with the increasingly blurred distinction between the politically-motivated activity of some terrorist groups and the criminal activities that fund them. Elements within Hizballah, Al-Qa'ida/the Taliban, Hamas, the former Liberation Tigers of Tamil Eelam and the Kurdistan Workers' Party operate or have operated criminal enterprises for profit or to advance their terrorist agenda.

---

71 Mrs Karen Harfield, Acting CEO, ACC, *Committee Hansard,* 17 February 2011, p. 8.

72 Det. Supt Charlie Carver, WA Police, *Committee Hansard,* 10 November 2010, p. 13.

> Other examples of such convergence have been noted by the UN Office on Drugs and Crime in Europe, South America and South-East Asia.[73]

2.83 However, the ACC has found little evidence of a convergence between terrorist groups and organised crime groups within Australia.[74]

2.84 Mr Kim Langton, Chameleon Associates, remarked that a security policy aimed at countering terrorist activity should naturally act to combat criminality, given the similarity in methods used. As he explained:

> The training that we give [clients] for counterterrorism picks up all the bits underneath, because you are going for the highest common denominator if you are looking for terrorists. If you are looking at that level you will pick up all the bits underneath and that includes criminal activities. The methodology that a criminal uses, whether it be in major crime or shop theft, is pretty well the same as what you would get from a terrorist. The method of operation, the way that they pre-plan, the way they do dummy runs, the way they actually do the act and the way they get away are all very similar. If you look at a military operation, it is very similar to the way that a terrorist operates. You are looking at one to five years to plan it and you are looking at the method that he uses and how he gets away. If you were to use a level of security that is up to catching terrorists, I believe you would be quite capable of picking up all the crime that goes on underneath.[75]

2.85 However, the Maritime Union of Australia (MUA) was concerned by the possible extension of MTOFSA beyond counterterrorism to a more general anti-crime stance, particularly in the context of the ASIC and MSIC schemes, discussed in Chapter 5. Mr Dean Summers, MUA, noted:

> We want to stress the fact that the unions throughout the whole process of the development of the Maritime Transport and Offshore Facilities Security Act, MTOFSA, and regulations, and any debate or discussion about security on the wharves or in areas of maritime endeavour in Australia—and that is in the offshore oil and gas, the ports and the ferries. They are partners in maritime security, primarily because internationally we know, through out International Transport Workers' Federation experience, that every time in every incidence of a terrorist attack transport workers are killed and hurt. So we have a vested interest and a responsibility to make sure that we are involved in the development of those instruments that protect or workers from these heinous crimes... [W]e are concerned that the focus of the entire debate is now shifting away from counterterrorism—and that is the whole reason we signed up to be partners in this—to what now appears to be countercrime.[76]

---

73 ACC, OCA 2011, pp 27–28.

74 ACC, OCA 2011, p. 29.

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

76 Mr Dean Summers, Maritime Union of Australia, *Committee Hansard*, 18 February 2011, p. 1.

2.86 On balance, the committee is of the view that aviation and maritime security policy does need to be extended beyond what appears to be a current, narrow focus on counterterrorism. The committee does not mean to argue that the current energy devoted to counterterrorism should be lessened, given the dire consequences of a successful terrorist attack. However, after a decade of national security policy development that emphasised counterterrorism, it is clearly in the national interest to extend those efforts to enhance the nation's ability to tackle serious and organised crime.

2.87 Specifically, the committee feels that the inclusion of serious and organised crime within the scope of aviation and maritime security legislation would be of benefit for three main reasons.

2.88 Firstly, as noted by the ACC, there is an increased risk of interaction between international criminal and terrorist organisations. Though this has not been observed within Australia, the extension of security legislation to cover both terrorism and serious and organised crime would further enable both to be treated as national security matters.

2.89 Secondly, criminal and terrorist organisations are able to exploit the same vulnerabilities within the aviation and maritime sectors. Protecting against criminal techniques will assist in preventing both criminal and terrorist activities.

2.90 Current transport security legislation is focussed on preventing a terrorist attack on aviation and maritime infrastructure itself. As a result, it may not capture the use of aviation and maritime trade and passenger routes to facilitate terrorist attacks outside of those sectors. For example, increasing the level of screening of air cargo could combat illicit drug importation and may also prevent a terrorist organisation from importing weapons or other dangerous items. Reducing vulnerabilities would eliminate opportunities for criminals and terrorists alike.

2.91 Finally, the threat of serious and organised crime alone warrants the enhancement of transport security legislation. For this and the above reasons, the committee recommends that the scope of key transport security legislation is widened to include serious and organised crime.

Recommendation 1

2.92 The committee recommends that the scope of the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003* be widened to include serious and organised crime in addition to terrorist activity and unlawful interference.

2.93 Through this recommendation, the committee would specifically like to improve the security plans developed under ATSA and MTOFSA. Importantly, the risk assessment and security plan required of airport and port operators would be extended to include an assessment and response to the threat of serious and organised crime. The committee understands that this would require a different set of threat

assessment skills compared to what is currently required. Nevertheless, the committee believes that this step alone would be extremely worthwhile and further involve the private sector in mitigating against the threat of serious and organised crime.

2.94 In Chapter 5, the committee recommends a number of changes to the ASIC and MSIC schemes that would complement the extension of those schemes parent legislation. The extension of those schemes would assist in preserving the integrity of the aviation and maritime sectors from criminal infiltration.

2.95 Finally, airport and port security committees, discussed in Chapter 3, would begin to discuss and review criminal threats. This would further engage the private sector in fight against the organised crime.

Tackling the issue: considerations

2.96 Over the course of this inquiry, the committee has visited ports and airports in most states and territories and spoken to a wide range of individuals and organisations operating in the aviation and maritime environment. This experience has led the committee to recommend a number of changes to security arrangements in those sectors, as described in the following chapters.

2.97 This inquiry has involved many of the same issues that occur in any law enforcement inquiry. Examples of perennial issues include the sharing of criminal intelligence, agency cooperation and the social and economic costs of increased security measures.

2.98 In addition, the committee has identified a number of issues particularly relevant to the aviation and maritime sectors, including the tension between commercial and security interests and the ease with which security measures could be circumvented through substitution of criminal methodologies.

The trade-off between security and commercial interests

2.99 A major theme of the inquiry is the inherent tension between commercial and security interests. Airports and ports are fundamentally areas of legitimate commerce. At the same time, their centrality to the movement of people and goods also make them areas of concern for national security and valuable targets for serious and organised criminal networks.

2.100 The sheer scale of trade, particularly through maritime ports provides some context to the complexity of tackling the subversion of legitimate trading routes for illicit purposes. Mr David Anderson, Ports Australia, observed that maritime trade was expected to double in the next decade, stating:

> Ports are often viewed, at least at community level, as a convening place for ships and seafarers, but of course they are in reality the largest freight hubs in the country. They are particularly significant in this country, of course, because we all depend on our trade-exposed economy. The growth in our container trades and our bulk trades, if our forecasting is right—and we

> believe it is probably understated rather than overstated—has our container throughput going up by about double GDP every year into the foreseeable future, which means, roughly speaking, a doubling of throughput in 10 years. We have some very big numbers in prospect in the bulk trades—our coal and iron ore trades, for example. Again roughly speaking, the throughputs will double in the next 10 years.[77]

2.101 To the extent that security measures inhibit the commercial viability of the sites, a trade-off exists between commercial and security concerns. Measures that reduce the productivity or commercial potential of the sectors may affect private companies and possibly the national economy.

2.102 One example that illustrates this point is the inspection of containers by Customs officials. The removal of containers for screening disrupts port operations to a certain extent. In addition to the direct cost of the screening operation, there is also an efficiency cost affecting the movement of containers. Increasing inspection rates beyond the current level of approximately 5 per cent[78] could serve to further deter the use of containers in illicit shipments, however it may also reduce the productivity of the port environment, with ramifications for the economy overall.

2.103 Another example, raised with the committee on a number of occasions during this inquiry, is the provision of commercial shopping outlets in airport security zones. While providing a service to customers and a commercial gain to operators, this practice also increases the number of people moving through secure areas, to the detriment of security. This was noted by Mrs Kathleen Florian, ACC, who stated:

> With both aviation and maritime, we are talking about streams that are absolutely critical to this nation's ongoing economy. We need to have passengers moving quickly and freely through airports. We need to be able to get our containers through [ports] quickly. There are very strong commercial interests that are absolutely critical for the nation. The balance between the passage of trade and people and the vulnerabilities is always a difficult balance to measure.[79]

2.104 In determining the correct mix of security measures in the aviation and maritime sectors, the committee has therefore had to balance legitimate commercial and economic interests with the committee's desire to combat serious and organised crime.

---

77 Mr David Anderson, Ports Australia, *Committee Hansard*, 18 February 2010, p. 48.

78 Customs, Annual Report 2007–08, p. 38.

79 Mrs Kathleen Florian, ACC, *Committee Hansard*, 17 February 2011, p. 13.

The potential for easy substitution

2.105 Another important issue affecting the committee's decision making was the degree to which a security measure could easily be circumvented by a change in criminal methods.

2.106 Security measures may be effective at addressing a particular vulnerability or known criminal method for which they were designed. However, the overall effectiveness of such a measure in disrupting serious or organised crime depends on how easily a criminal network can turn to an alternate method of achieving their aim.

2.107 For example, if security was improved at one airport or port in isolation, it may be a simple matter for a criminal network to reorient its distribution or importation network to use a different airport or port. Another example provided to the committee was the use of general aviation airports for the distribution of illicit drugs. If security was improved at such airports to the extent that it was no longer practical to use the facilities for criminal activity, criminal organisations could potentially use nearby unregulated landing strips. Alternately, other methods of transport including cars, trucks and trains could be adopted.

2.108 Mr Michael Phelan, Deputy Commissioner of the AFP elaborated on the potential for method substitution, stating:

> [O]rganised crime groups are dynamic, flexible and risk averse and will seek alternate methods of transporting illegal goods in and out of Australia. With its large coastline and vibrant mining industry, Australia's remote industrial ports remain vulnerable to exploitation by organised crime groups. Similarly, the use of small rendezvous type craft to convey illegal goods from offshore mother ships to non-commercial ports is a known methodology for avoiding law enforcement interest. The recreational cruise ship industry also represents some additional opportunities for infiltration by organised crime. These examples clearly illustrate that the focus of law enforcement must remain on serious and organised crime in its broadest sense. If attention is directed at one environment to the detriment of the bigger picture, organised crime groups will quickly circumvent law enforcement detection. This will result in the problem being displaced and not necessarily defeated.[80]

2.109 This is not to argue that a security measure is not worthwhile simply by virtue of another potential criminal method. Targeting the most lucrative methods may force criminal organisations to use more costly or less efficient methods, undermining the viability of criminal activity, reducing profit and commensurate incentive. Furthermore, criminal organisations may be forced to use riskier methods that are more amenable to discovery by law enforcement agencies.

---

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

2.110 At the same time, the committee is also of the view that certain, minimum security requirements are desirable, even if they can be circumvented by serious and organised criminal networks. The ACC investigations into the aviation and maritime sector also identify the existence of low-level, opportunistic crime, which does stand to be significantly disrupted by minor security improvements. This was a view shared by Mr Richard Janeczko, who argued:

> I think the other thing is that a lot of major crimes are committed by disorganised criminals, not only organised crime. Some of these people who are making millions and billions out of the Commonwealth are not that well organised. Sure, you will not get some of the so-called Mr Bigs, but I do not think that is a reason not to make the border as secure as it can be.[81]

2.111 The committee has sought to be mindful of this 'substitution issue' in coming to conclusions of this report.

Capturing the entire supply chain

2.112 The majority of significant organised crime at airports and seaports involves the trafficking of illicit goods, most commonly, drugs. The importation and distribution of such illicit commodities involves a logistical chain just like any licit importation. It is therefore essential that measures to combat serious and organised crime target the supply chain as a whole, and not just the airport or seaport.

> Our focus, and it flows from the purpose of the act, is on the ship to shore interface. At a port we focus on the actions of port facility operators, stevedores and port service providers. We do not have a focus on whole of supply chain in the maritime sector, which is where you are going, as I understand it.[82]

2.113 The ACC observed a discrepancy in the treatment of various aspects of the overall supply chain, writing in its submission to the inquiry:

> Although interlinked with issues relating to broader inter-modal transportation, maritime and air cargo is subject to a security regime that weakens as the goods move further down the cargo movement chain. Theft from bonded or packing/unpacking warehouses is not uncommon and was often not reported to law enforcement agencies, even when losses were apparent or persons of interest started to emerge. Often it is unclear where and when in the supply chain that theft has occurred.[83]

2.114 As Mr Michael Phelan, Deputy Commissioner, AFP, noted:

> ...[W]hen we are talking about serious and organised crime at the ports and the investigation of that crime, the ports are but a small component of that. If we are talking about a container or any sort of commodity, it is where it

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

82 Mr Paul Retter, OTS, *Committee Hansard*, 18 February 2011, p. 42

83 ACC, *Submission 8*, p. 12.

> passes through. It is not necessarily organised or facilitated there; it is one of the points in the supply chain to get drugs from the Golden Triangle all the way to the streets of Sydney or somewhere like that. It is one of the many components that are worked through. That is what the Australian Federal Police and our law enforcement partners are working on—not just that one particular point in the supply chain, but everything else. The vast majority of activity that comes through the ports actually operates outside of the ports.[84]

2.115 This point was also made by various witness groups in the context of the ASIC and MSIC schemes, with arguments made to extend that measure, which aims to safeguard the integrity of workforces, to other equally key areas of the supply chain.

2.116 The committee notes the importance of a 'whole of supply chain' approach that focuses on the broader aviation and maritime sectors.

2.117 More broadly again, security measures enacted at airports and ports must match broader law enforcement efforts to tackle organised crime. For example, officers and teams working at airports and ports need to liaise regularly with police organised crime units. Airports and ports are simply one part of a complex supply chain, and it is the supply chain itself that is of value to SOCNs.

Two approaches to combating serious and organised crime

2.118 The committee has identified two main approaches to combating serious and organised crime in the aviation and maritime sectors. The first is referred to by law enforcement agencies as 'hardening' the environment. This involves instituting measures that make it harder for SOCNs to use those sectors for criminal purposes. Measures discussed in other chapters include ensuring the integrity of workforces, physical security and screening and detection regimes.

2.119 The second is active disruption of SOCNs by law enforcement agencies. In particular, this requires the use of information, including criminal intelligence, to guide investigations and tactical operations as well as strategic policy responses. Accurate and regular intelligence analysis is essential to combating serious and organised crime as it enables the targeting of scarce policing resources to the area of highest risk. This can include successful operations to seize illicit shipments and dismantle networks. It can also involve the development of understanding of how criminal activity is occurring, guiding effective policy responses. The use of criminal intelligence is central to the concept of 'intelligence-led' policing.

2.120 The committee considers that both of these approaches are important, but particularly emphasises the second. The use of intelligence and the facilitation of

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

cooperation and information sharing is vitally important in strengthening the law enforcement response to organised crime, regardless of the methodology adopted by criminal networks. This approach is discussed in the next chapter.

2.121 By contrast, 'target-hardening' measures suffer from the substitution effect identified above. As a result, these measures need to be closely examined to ensure that the disruptive effect is substantial enough to warrant the expenditure required as well as economic and social costs required. These approaches are discussed in Chapter 4.

2.122 The report concludes with an examination of the ASIC and MSIC schemes in Chapter 5.

Chapter 3

Intelligence and Cooperation

Overview

3.1 Over the course of this inquiry, following discussions with law enforcement agencies around Australia, the committee has come to the view that the use of intelligence is vital in directing operations targeting organised criminal activity generally, and specifically in the aviation and maritime sectors.

3.2 Secondly, the coordination of the law enforcement response, including the conduct of investigations, operations and policing are also important. Intelligence and information-sharing is a necessary part of such coordination. This chapter examines the current intelligence collection and sharing approaches, as well as the specific agency coordination arrangements in the aviation and maritime environments.

3.3 The following sections describe the evidence heard and the committee's findings in relation to law enforcement models at Australia's airports and ports. This involves two separate but related elements. The first is the coordination of policing and security: the physical presence provided at ports and airports and elsewhere in the aviation and maritime sectors, either in the form of uniformed officers or private security. The second relates to the coordination of information; the mechanism by which relevant stakeholders are able to share information in order to inform the response to criminal threats.

Coordination of law enforcement agency activity to combat serious and organised crime

3.4 Australia's law enforcement response to the threat of serious and organised crime involves a number of agencies and requires that they work together. At the Commonwealth level, the AFP and ACC work as key partners, with both agencies working collaboratively on investigative and intelligence responses to organised crime.[1] Given the international nature of organised crime, the Customs and Border Protection Service naturally has a key role to play in preventing the movement of illicit goods across national borders.

3.5 Commonwealth agencies must also work together with state and territory police. Given the different jurisdictions of the various police forces, it is important to coordinate activity so as not to cause any gaps or significant overlaps in police activity. As Mr Richard Janeczko noted, the different powers and focus between agencies requires the close cooperation of each to ensure that those powers and skills complement one another, stating:

---

1 Australian Federal Police, *Submission 19*, p. 2.

> Customs no longer has some of the powers that it used to have—things like executing a three year warrant under the Criminal Code. Customs does warrants in its own jurisdiction and, if there is enough evidence, in discussion with the DPP it will become a criminal prosecution. Customs does not have the ability to access TI, telecommunications intercept, material. Customs is an armed investigative body as well as a border protection body, yet it has a restriction on how well an investigation can be carried out, because it has to go to other agencies to get the normal tools that people doing that kind of work should have. You would have to go to the AFP or the Crime Commission to continue an investigation.
>
> Liaising is getting better and it is important, but the trouble is that a lot of the agencies we are talking about are overstretched anyway. It was not unusual in most of my years in investigation that, if I asked another agency if they would like to help me, they would say, 'Come back in three weeks time, on Monday week or a month's time and then we will help you.' That does not help you much if the container is leaving. We will use the state police if we can. We get a lot of cooperation but, at the end of the day, other agencies' priorities are not ours.[2]

3.6 These issues have been raised by the committee before, and continue to be addressed through a number of cooperative arrangements. The focus of this inquiry has been on the specific coordination mechanisms in place in the aviation and maritime sectors. The current arrangements are described below.

Airport law enforcement coordination arrangements

3.7 Major airports have had a uniformed police presence for many years, given the high volume of people passing through the facilities and the resulting need for community policing services. Similarly, in the post-September 11 environment, there has been a need for a counter-terrorism response. However, the exact nature of policing at airports has changed over those years.

3.8 In recent times. airport policing arrangements at the major airports have been significantly influenced by both the Wheeler Review and the Federal Audit of Police Capabilities, conducted by Mr Roger Beale AO (Beale Audit).[3] The Wheeler Review specifically identified three areas of concern relating to airport security and policing culture at major airports. These included:

- a marked inhibition about sharing information with those who need it to make evidence-based decisions;
- a lack of clarity, consistency and alignment between authority and responsibility in decision-making; and

---

2 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 18.

3 Mr Roger Beale AO, Federal Audit of Police Capabilities, June 2009, http://www.ema.gov.au/www/agd/agd.nsf/Page/Publications_FederalAuditofPoliceCapabilities (accessed 10 June 2011).

- an undue reliance on 'after the event' compliance auditing, rather than 'pre-event planning' as the basis for accountability.[4]

The Universal Policing Model

3.9 Following the 2005 Wheeler Report, the Commonwealth Government instituted a 'Unified Policing Model' (UPM) at Australia's 11 major airports. The UPM involves a mix of federal, state and territory police being responsible for policing at airports in a cooperative framework. The UPM is delivered through a centrally coordinated command structure using both AFP and seconded state and territory police.[5] Under the UPM, the unified policing presence includes:

- Airport Police Commanders;
- Police Aviation Liaison Officers;
- Airport Uniform Police (which include state and territory police seconded to the AFP);
- Joint Airport Intelligence Groups (JAIGs);
- Joint Airport Investigation Teams (JAITs); and
- a Counter-Terrorist First Response (CTFR) capability.[6]

JAITs and JAIGs

3.10 A key feature of the UPM was the establishment of, Joint Aviation Intelligence Groups (JAIG) and Joint Aviation Investigation Teams (JAIT) at major airports. Membership of these groups could potentially include officers of the AFP, state or territory police, Customs, Australian Quarantine Inspection Service (AQIS) and the ACC. As Mr Jeff Buckpit, Customs, explained:

> The role of the JAITs and JAIGs at the airports is to investigate matters, whether they be criminal or otherwise, of concern to law enforcement. The teams that we are talking about are typically fairly small, of the order of 10 people. Typically, you are looking at representation from the AFP, state police and Customs. Sometimes there is participation from other agencies on an as-required basis. The JAIT function is investigative. The JAIG function is an intelligence support role. Both teams are quite small. I think it is in five international airports that we have the JAITs and JAIGs. Their role is certainly a key role in terms of organised crime and issues of infiltration.[7]

4 Wheeler Review, p. 33.

5 AFP, *Submission 19*, p. 3.

6 AFP, *Submission 19*, p. 3.

7 Mr Jeff Buckpitt, Australian Customs and Border Protection Service, *Committee Hansard*, 17 February 2011, p. 4.

3.11 Mr Richard Janeczko informed the committee they had at least improved the flow of information between the agencies, stating:

> I am not sure whether the committee is aware that the model as it was introduced did not have any impact apart from the beneficial interchange of intelligence to the operations of Customs investigation and prosecution. The airport model does not mean that Customs then stepped away and the AFP conducted its investigations into whether it was child pornography, tobacco smuggling, firearms or whatever. That continues and I think it works very well. The airport model did provide a greater forum for the interchange of intelligence and a better way to create taskforces.[8]

3.12 Mr Michael Phelan, Deputy Commissioner of the AFP, informed the committee that the UPM, together with the JAIT/JAIG model had improved the policing response to organised crime in airports, stating:

> In addition to the provision of law and order and general security, the unified policing model provides multijurisdictional investigative capabilities to the joint airport investigation teams and the joint airport intelligence groups. This affords a policing response to airport based organised crime that is linked to broader law enforcement activities focused on related criminality external to the aviation environment.[9]

3.13 The committee gained a generally favourable impression of the JAIG/JAIT model. In particular, it would seem to provide a useful mechanism for the sharing of intelligence at a tactical or operational level within the airport environment. It is, however, limited to five major airports.

3.14 However, not all witnesses believed that current arrangements were working. Mr Michael Carmody, who appeared before the committee in 2009, commented on the confusion that continued to arise from the multitude of law enforcement organisations operating at the airport, stating:

> One of the exercises that fall out of this is that you go to Sydney airport and you have Customs, who have certain powers, you have AQIS, who have certain powers, you have the airport operator, who under the aviation act has certain powers, you have Qantas, who have certain powers as the aircraft operator, you have the Qantas security force, which actually has no power, you have New South Wales Police and you have the Federal Police. They are all in amongst this mix with no-one truly overarching that in control with respect to the management of that function. Yes, there are security programs constructed at each airport and, yes, the airport operators have a responsibility with respect to the coordination of that exercise but it is a monster beyond belief. And of course you have got Customs, who did not wish to do or share, you have got AQIS, who do not wish to do or share, you have got the airlines and airport operators, who have their agendas, you

8 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 14.

9 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 38.

> have got New South Wales Police, who have been overworked from day one, and you have got the Federal Police, who have a role associated with Customs and AQIS but will step into the breech if necessary. I just do not understand it and never have.[10]

3.15 The committee notes that since Mr Carmody's appearance, the policing model has changed to consolidate more responsibility under the AFP.

Movement to an 'All-in' model

3.16 In December 2009, the Minister for Home Affairs, in response to the Beale Audit's examination of the AFP's capacity to meet future needs, announced a move to an AFP-led 'All-in' policing model. The Beale Audit had recommended the Commonwealth:

> …vigorously pursue the replacement of the existing Unified Policing Model with an 'All In' model under which the Commonwealth accepts the responsibility of funding and staffing nationally coordinated airport security and policing services, noting that this will likely take several years before being fully operational. It should take any legislative action, or pursue the renegotiation of arrangements in a number of states and territories, to ensure that the powers of AFP members policing airports are clear and adequate to the task.[11]

3.17 The All-in approach will see the AFP becoming responsible for staffing airport policing services at the 11 major airports. This entails a staged move over five years to a fully-sworn AFP capability instead of the current mixed Commonwealth and state policing model.[12]

Use of private security

3.18 In addition to the uniformed police and customs presence at major airports, private security arrangements remain an important element of airport security. Private security forces are responsible for screening passengers entering 'sterile' secure areas as well as maintaining perimeter security in restricted areas.

3.19 Both union submissions and Mr Michael Carmody expressed concern that the continued outsourcing of private security, based on a least-cost tendering, contributes to overall security vulnerability. The Transport Workers Union informed the committee that high turnover of security guards meant that up to 25 per cent of operated using a Visitor Identification Card, rather than a full background-checked

---

10 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 10.

11 Mr Roger Beale AO, Federal Audit of Police Capabilities, June 2009, p. 12.

12 The Hon. Brendan O'Connor, 'Australian Federal Police to Lead Airport Security Across Australia', *Media Release*, 29 December 2009.

Aviation Security Identification Card.[13] This particular concern is addressed in Chapter 5.

3.20 The TWU were also investigating allegations that a lack of sufficient training of contract baggage handlers was resulting in a proportion of baggage not being X-rayed prior to placement on aircraft. Mr Anthony Sheldon, TWU, particularly singled out the issue of subcontracting by security firms as a risk to security, stating:

> The last count we had we could identify 12 private security companies out at the airport. Those are the ones we can identify, because, even though they are subcontracted twice or three times down, they will be wearing the same shirt from the principal contractor. We have raised it on numerous occasions. When you have high staff turnover, you have not only a lack of vigilance, but poor training. Mature age training involves not only training in a training room but also of course involves experience on the job from well-trained mentors. If you have a high turnover that does not involve any training, that does not have a mentor system because of the high turnover, then you will have staff that are poor performers. It also means, of course, that at our airports with those different contracting levels, because the wages are low, the conditions are poor, there is a high turnover and with high turnover means higher risk.[14]

3.21 This point was echoed by Mr Mark Padget, WA Police, who stated:

> One of the subcontracting issues that we came across was the ability of, say, the major contractor to devolve parts of his contract obligations to a subcontractor while not passing on the obligations of his original contract. There is some blurring of the lines in terms of levels of service and levels of commitment to what level they screen, what training they have and even down to the types of people that have the ability to hold a security agent's licence.[15]

3.22 High turnover places stress on training structures, while increasing the number of new people flowing through the aviation sector. As the Australian Services Union (ASU) described:

> In summary, our view is that a happy, long-term, well-paid workforce is going to be a significant factor in how security is dealt with at airports. We certainly believe that and that has been our experience. High turnover and casualisation, adds further complexities to the workforce and also exposes security concerns.[16]

---

13 Mr Anthony Sheldon, Transport Workers Union of Australia, *Committee Hansard*, 18 February 2010, p. 61.

14 Mr Anthony Sheldon, TWU, *Committee Hansard*, 18 February 2010, p. 55.

15 Mr Mark Padget, Western Australia Police, *Committee Hansard*, 10 November 2010, p. 12.

16 Ms Linda White, Australian Services Union, 17 Feb 2010, p. 8.

3.23 Mr Stephen Jackson, Qantas, informed the committee that it never allowed subcontracting by the security companies it hired, stating:

> The only time that we would permit subcontracting under contract is if the primary contractor—which would be ISS, MSS or SNP Security—sought out permission to do so. They have in the past sought out permission and we have denied that permission. I want to be very clear and say that there are no subcontracted security officials on any Qantas location in any airport in Australia.[17]

3.24 Mr Kim Langton, Chameleon Associates (Australia), expressed a strong preference for a government-run security force at airports, similar to the Aviation Security Service (Avsec) model used in New Zealand. Mr Langton commented that the Avsec model benefited from having staff employed under a single umbrella, with harmonised training, high pay and very low turnover. By contrast, contracted private security faced a number of issues, as Mr Langton explained:

> As a contractor working for either the airport or the airlines, you have to remember the contractor has to make money. To do that means that the training he supplies and the level of service he supplies will not be as good as they would be if it were run by a government body. If you look at the airports at the moment and the civilian contractors that are there, your turnover is massive. They have major problems with sick days, people working double shifts and it has even got to the point with some of the contractors that we have [subcontractors] working for the contractors. I just do not think that is the way to go.[18]

3.25 Mr Langton noted that through the transition to the All-in policing model, a number of trained AFP Protective Service Officers would become redundant. He was of the opinion that this body of officers could form a competent government-run security force at airports.[19]

> It always beggars belief, in my view, that with respect to Customs and AQIS the government has no hesitation or limitation in taking full control and management of those functions within the national interest. They are staffed by government employees, they have good technology and infrastructure in place, airports and ports are built around the function, and the staff are reasonably well-paid and reasonably motivated. The exact opposite exists in aviation security, and I do not understand that. Why does the government step back from the third leg of that stool of border protection, and yet the focus on AQIS and Customs is a given. I do not understand.[20]

---

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

18 Mr Kim Langton, Chameleon Associates (Australia), *Committee Hansard*, 18 February 2011, p. 54.

19 Mr Kim Langton, Chameleon Associates (Australia), *Committee Hansard*, 18 February 2011, p. 59.

20 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 4.

3.26 Mr Carmody elaborated on the privatisation of federal airports since the days of the Federal Airport Corporation, stating that while security had not been 'spectacular' under that system, it was stable and suitable. In Mr Carmody's words, following privatisation:

> In that shift to privatisation, of course, the new owners came in and airport operators immediately devolved that responsibility to airlines and got out of the security game because it was just too expensive. Airlines said, 'We're not going to wear this,' so they immediately outsourced it to a private security company and, generally, to the company that provided the tender at the lowest cost. Everyone simply transitioned the risk through that process, so what you have now, be it at regional airports or at domestic airports, including international, is private security companies at the absolute end of the chain bearing the risk for the entire profile of aviation security.[21]

3.27 The committee is deeply concerned by the potential for security lapses as a result of the high turnover of staff, particularly security guards. The committee is therefore agrees with arguments that private security at airports should be replaced with a government security force, as has occurred in some other countries.

3.28 Accordingly, the committee recommends that the security at the 11 major airports be undertaken by a suitably trained government security force. In implementing this recommendation, the committee suggests that the Commonwealth government be informed by both the American and New Zealand aviation security models.

Recommendation 2

3.29 The committee recommends that security at major airports be undertaken by a suitably trained government security force.

Airport security committees

3.30 Sydney Airport Corporation Limited (SACL) informed the committee that since the Wheeler Review, airport security committees had been established at major airports. This committee was the leading body at the airport for the organisation of security measures, and included agencies such as the ACC, ASIO and other law enforcement or intelligence agencies.[22] The airport operator had a leading role on that committee, as explained by Mr Grant Woods, SACL, who stated:

> We chair that committee. It is there primarily to share intelligence on various activities that may be going on with a Federal Police operation or an Australian Crime Commission operation. It has a format that reviews, for example, the full risk register that is applied across the airport, which is

21 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 8.

22 Mr Grant Woods, Sydney Airport Corporation Ltd., *Committee Hansard*, 18 February 2010, p. 13.

> obviously intelligence based on the vulnerabilities that we see at the airport itself.[23]

3.31 Later in the same hearing, Mr Woods elaborated further, stating:

> That committee... reviews the risks for the airport every two months. If the Crime Commission or the police state that there is an issue that they are dealing with, we will discuss that at that table and we will develop measures and plans to deal with that issue as a risk.[24]

3.32 The airport security committee model is established through the ATSA legislation discussed in Chapter 2. As such, it is geared towards the prevention of a terrorist attack. The JAIT and JAIG model however focuses on all serious and organised crime.

3.33 As a consequence of the committee's first recommendation that ATSA be expanded to include consideration of the threat of serious and organised crime, airport security committees would take on an enhanced role. By considering both terrorist and criminal threats, the role of the airport security committee would become more meaningful and involve key airport stakeholders in the mitigation of organised criminal threats.

Port law enforcement arrangements

3.34 In marked contrast to the airport environment, port security is generally a private concern, with little in the way of a permanent police presence. Individual companies are responsible for contracting private security guards, in line with an agreed maritime security plan. This results in a number of separate, private security forces on the waterfront. Some submitters and witnesses have suggested that the establishment of a single, centralised security force may improve overall security outcomes.

3.35 The Australian Customs and Border Protection Service (Customs) also maintains a presence at major ports, in the form of randomised patrols,

> Our environment encompasses the maritime domains of our exclusive economic zones, seaports, airports, international mail centres and cargo depots and warehouses. The Customs and Border Protection Service does take a leading role in combating serious and organised crime at the border, through targeting, detecting and interdicting illegal cross-border movements of people, goods, vessels and aircraft. We investigate border offences and regulate certain entities operating in the border environment through licensing depots, warehouses and customs brokers.[25]

---

23 Mr Grant Woods, SACL, *Committee Hansard*, 18 February 2010, p. 13.

24 Mr Grant Woods, SACL, *Committee Hansard*, 18 February 2010, p. 21.

25 Mrs Marion Grant, Deputy Chief Executive Officer, Customs, *Committee Hansard*, 17 February 2011, p. 2.

3.36 Customs officers also board all 'high to medium risk' commercial vessels arriving from overseas within one hour of their arrival.[26]

3.37 As most major ports are state corporations and ports are generally a state jurisdiction, the burden of formal policing falls to state police forces. However, the AFP notes that it is involved in the investigation of a range of criminal groups that may exploit maritime security. The majority of AFP involvement in ports relates to the use of legitimate sea cargo to import or export illicit goods.[27]

3.38 The Australian Federal Police Association remarked upon the apparent confusion regarding responsibility for policing at major ports in Australia. As Mr Jonathan Hunt-Sharman observed:

> I can assure you that, in regards to a permanent police presence at key maritime ports, there are no Australian Federal Police there. In fact, a number of us who have worked over the years in drug investigations have been quite amused by that comment because we have hardly been on the cargo ports themselves. There is clearly a gap that is sitting under the radar that has not been addressed. Some people think there are state police there, but when the state police give their statements they say, 'No, it is the Australian Federal Police.'[28]

3.39 The Australian Federal Police Association (AFPA) argued in favour of replicating the 'All-in' policing model currently under development at airports in the maritime environment.

> The AFPA believes that the Commonwealth government should pursue the replacement of the existing maritime security structure with an all-in model under which the Commonwealth would assume responsibility for the coordination of maritime security and policing services at key maritime general cargo ports such as Sydney, Melbourne, Brisbane and Fremantle. In the event of such a change, the expansion of the AFP to include responsibility for maritime security and policing would make sense as a natural flow-on from its jurisdiction of Australia's major airports. Many of the recent recommendations arising from the federal audit of police capabilities conducted by Mr Roger Beale AO, which are partly aimed at streamlining the aviation security structure, could equally be applied in the context of the maritime industry.[29]

3.40 The AFPA also recommend the use of AFP Protective Service Officers to supplement private security guards, establishing a permanent uniformed presence at major ports. Mr Jonathan Hunt-Sharman elaborated on this proposal, explaining:

---

26 Customs, *Submission 13*, p. 9.

27 AFP, *Submission 19*, p. 6.

28 Mr Jonathan Hunt-Sharman, Australian Federal Police Association, *Committee Hansard*, 17 February 2011, p. 30.

29 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, pp 25–26.

> The important thing in regard to the AFP Protective Service officers is the fact that they are sworn officers that are under the full AFP integrity regime and they are highly trained. What it would do is that, whilst they are playing a role of protecting the security of the area, they would become the eyes and ears and the conduit for information to be passed through to the AFP.[30]

3.41 AFPA put the cost of providing for providing 30 PSOs at a single port, plus supply costs, at approximately $5.1 million per annum, while replicating the JAIG/JAIT model at a port was estimated to cost $6.1 million per annum.[31]

3.42 The AFP noted a distinction in the requirement for community policing between the airport and seaport environment. Mr Phelan explained:

> The maritime space is a different environment to those that we have at the airports, because the airports are about people. There are lots and lots of people moving through an airport, and normal criminal offences occur to them. The seaports are a different kettle of fish. There it is about commodities, with sea containers and so on. Most of the people that are there are the employees who are working on the docks. In terms of normal criminal activity, it is difficult to ascertain what is being reported and underreported. There would be more criminal activity in terms of volume at an airport, probably, simply because of the volume of people that go through, than there would be at a port. There I am talking about normal criminal activity, not serious and organised crime, because we are well and truly aware of the vulnerability of the ports given that they are one of the major avenues where illegal goods come in.[32]

3.43 Customs also noted that the differing needs of the port and airport environment meant that a simple replication of the airport unified policing model at a seaport would not be straightforward.[33] Mrs Grant noted that, while difficult in practice due to the needs of busy seaport, there was perhaps potential for strengthening the legal framework surrounding ports, stating:

> But we would say that the legal framework around the seaports is less robust than in the international airport environment. Take Customs controls around seaports. We gazette, under section 15 of the Customs Act, a seaport and then that becomes a Customs-controlled area. But if you look at the provisions within that section of the Customs Act, you see we do not have huge powers within that act to do many things apart from set some parameters about what can and cannot be done with cargo in the area. They do not necessarily give us the same level of control that we have over access to areas in international airports. From that point of view from the

30 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 27.

31 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 27.

32 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, pp 41–42.

33 Mrs Marion Grant, Deputy Chief Executive Officer, Customs, *Committee Hansard*, 17 February 2011, p. 3.

> framework of stronger controls, we would certainly see that there is scope technically to do something.[34]

3.44 Mr Richard Janeczko was of the opinion that rather than giving responsibility to a single agency, the key was the cooperation of the multitude of agencies involved, stating:

> At the end of the day it is all about cooperation, sharing of intelligence and setting up taskforces when they need to operate. I do not think that just creating a structure that is called a unified policing model is necessarily the answer even though that is a good way to encapsulate it. The airport model works mainly because of the cooperation between the agencies involved and the fact that a number of agencies contribute to it. I think you have to be very careful of putting a sort of umbrella organisation in charge of everything, I think we need to understand what that means before we try to do that in a maritime environment.[35]

3.45 Recently, the AFP, Customs, ACC and the NSW Police announced the establishment of the Port Crime Task Force, which will initially focus on crime in the NSW maritime sector.

> Operational members from the AFP serious and organised crime portfolio occupy senior positions within joint taskforces the remit of which includes criminality at the ports. Working closely with colleagues from the ACC and Customs and the New South Wales Crime Commission, these members focus on the nexus between organised crime entities and the maritime port environment in New South Wales. These taskforces have enjoyed a number of operational successes and have contributed to a better understanding of the criminality in Australia's ports.[36]

3.46 The AFP were of the opinion that information sharing between agencies working at seaports, particularly of intelligence, had improved significantly over the last two years. Mr Phelan noted:

> We have been directly related to this over the last couple of years, and I do not think I have ever seen the intelligence exchange between the agencies more joined up than it is now at our seaports, particularly the relationship between the AFP and the Customs and Border Protection Service, as well as the state police... [S]ince the submission was first done, in 2009, we have come a mile and a half in terms of working with our state partners, particularly in the sharing of intelligence.[37]

---

34 Mrs Marion Grant, Deputy Chief Executive Officer, Customs, *Committee Hansard*, 17 February 2011, p. 3.

35 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 15.

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

37 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 42.

3.47 Mr Phelan also informed the committee that the AFP hoped to establish the New South Wales Port Crime Taskforce model to other states:

> There are protocols that exist between the Australian Federal Police and Customs and each of the state police agencies about the sharing of intelligence within the seaports, and we are actively working with our other partners at the moment, in states other than New South Wales, to form joint task forces at the seaports similar to the arrangements that exist at the airports around the Joint Airport Investigation Teams and the Joint Airport Intelligence Group but, quite frankly, far more robust—in other words, with more people and better resourced to meet the threat. That is the key thing, in our view, around the seaports. Intelligence is the key.[38]

3.48 The committee took the opportunity at hearings to explore the potential for mirroring the JAIG and JAIT structures in the seaport environment, to facilitate the sharing of information and intelligence, thereby strengthening investigative and analytical functions. Mr Jeff Buckpitt, Customs, noted that the creation of taskforces such as the NSW Port Crime Taskforce were in fact intended to achieve similar aims, albeit for a particular period of time and for a particular purpose.[39] Mr Buckpit elaborated on the potential for a formal structure copying the JAIT and JAIG functions, stating:

> I think that there would be pros and cons. The fact that the port environment is so physically different from an airport's is part of the consideration that makes the question fairly complex. Take just the issue of accessing containers. Most of the containers are accessed away from the actual port environment. There are exceptions to that, of course, but for the most part there is the fact that they are accessed away from the port environment. If you were to have a JAIT type of operation at a seaport, you would have to think carefully about what their role would be, because they would not be doing the sorts of things that Customs is currently doing in terms of opening up containers at our container examination facilities.[40]

3.49 The AFPA supported the introduction of a JAIT/JAIG model at maritime ports, stating:

> [A] model similar to the JAIT's and the JAIG's could work very well with the state police. It gets around a lot of the jurisdiction issues. Those models in aviation have been very successful and can quite easily be replicated, we would argue.[41]

3.50 The committee is firmly of the view that a specific agency coordination model is required at ports. The committee's preferred model emulates the functions of the

---

38 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 42.

39 Mr Jeff Buckpitt, Customs, *Committee Hansard*, 17 February 2011, p. 4.

40 Mr Jeff Buckpitt, Customs, *Committee Hansard*, 17 February 2011, p. 4.

41 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 30.

JAIGs and JAITs at Australia's major airports. The committee recommends that permanent taskforces mimicking the intelligence sharing and investigation functions undertaken by JAIGS and JAITs be established in every state. The taskforces should properly focus on those ports assessed as being of highest risk by the ACC. Nevertheless, taskforces should be familiar with other elements of the maritime sector, including minor ports, as necessary.

3.51 These joint taskforces should include officers of the AFP, state or territory police, Customs and the ACC at minimum. The taskforces would necessarily work closely with state and federal police organised crime units.

Recommendation 3

3.52 The committee recommends that joint maritime taskforces, mirroring the functions of the Joint Aviation Investigation Teams and Joint Aviation Intelligence Groups in the maritime sector be established in every state and the Northern Territory. These taskforces should include officers of the Australian Federal Police, state or territory police, the Australian Customs and Border Protection Service and the Australian Crime Commission.

3.53 In addition, the work of the state-based squads will need to be coordinated nationally. In part, this will be achieved through the participation of Commonwealth officers, who will be responsible for bringing the corporate knowledge of their home agencies to the joint maritime taskforce.

3.54 However, the committee is of the opinion that the work of the state-based taskforces should be supplemented by Commonwealth maritime crime taskforce arrangement. The national taskforce would comprise leaders of the state taskforces and could meet on a regular basis to ensure that knowledge was not siloed in any particular state.

3.55 The committee also recommends that this national coordinating body be assigned a cross-agency group of officers that could act as a national maritime 'flying squad'. The term 'flying squad' refers to a mobile group of officers who are able to move to areas requiring attention as needed. In this case, a Commonwealth maritime flying squad, led by the AFP, could concentrate expertise on particular ports in response to particular intelligence, assisting state-base taskforces. Additionally, a flying squad could conduct randomised audits of maritime security. This would provide an additional layer of scrutiny and a further disincentive to criminal activity in the form of a heightened risk of detection, even in smaller ports.

Recommendation 4

3.56 The committee recommends the formation of a Commonwealth maritime crime taskforce that would act as a national Australian Federal Police led 'flying squad', responding to specific intelligence and also conducting randomised audits of maritime and seaport security.

Port Security Committees

3.57 The MTOFSA legislation provides for the establishment of a Port Security Committee, which includes most relevant port stakeholders, such as the AFP, state police, terminal operators, the Navy, Customs and AQIS.[42]

3.58 The primary role of the committee is to discuss the implementation of maritime security plans, which are based on preventing terrorism.[43] As a result, in their current form they do not fulfil the same function as the JAIG/JAIT model at airports which focus more broadly on serious crime.

Intelligence-led policing

Introduction

3.59 The sharing of information, specifically intelligence, goes hand in hand with a cooperative approach to policing and law enforcement. The various policing models, either current or proposed, outlined above aim to ensure coordination of action and the necessary flow of information between agencies.

3.60 Intelligence can be used in two distinct ways. Firstly, intelligence about criminal activity can be used at a tactical level, to inform law enforcement operational responses. Examples of this in action include the many drug seizures resulting from tip-offs and other intelligence sources.

3.61 However, intelligence can also be used at a strategic level, using analysis to identify criminal patterns, thereby informing the policy response and high-level agency approaches. Examples of this type of work can be found in the ACC's various intelligence products. By analysing the full range of existing intelligence, governments can address systemic vulnerabilities, reducing criminal opportunity.

Intelligence-led operations

3.62 The committee notes that many successful operations that significantly disrupt organised criminal activity, such as large drug seizures or the dismantling of particular networks rely on quality intelligence. All law enforcement agencies before the committee noted the importance of intelligence in this regard, and the importance of information sharing as a result.

3.63 The AFP explained that cooperation between partner agencies allowed combined targeting of groups in response to intelligence, submitting:

> The AFP maintains close working relations with various government agencies including Australian Fisheries Management Authority (AFMA), Customs and Border Protection, [the Australian Maritime Safety

42 Mr Shane Hobday, Sydney Ports Corporation, *Committee Hansard*, 18 February 2010, p. 41.

43 Mr Shane Hobday, Sydney Ports Corporation, *Committee Hansard*, 18 February 2010, p. 42.

> Authority], and AQIS for example. In particular, the AFP maintains a close relationship with Customs and Border Protection in respect to strengthening border controls and increasing detections of illicit goods; sharing intelligence derived from investigations and identifying organised crime syndicates for joint or individual targeting.[44]

3.64 Mr Michael Phelan, Deputy Commissioner of the AFP, elaborated further at a committee hearing, explaining that the use of intelligence increased the effectiveness of the law enforcement response, stating:

> Criminal intelligence is used to inform, prioritise and plan all AFP operations. The active gathering of intelligence on organised crime groups improves investigational effectiveness and efficiency and allows law enforcement to be both proactive and opportunistic, targeting vulnerabilities in criminal groups and their methodologies. The AFP works closely with partner law enforcement agencies, including the ACC with its coercive powers, to develop an increasingly detailed intelligence picture of organised criminality, including at air and sea ports.[45]

3.65 Customs expressed a similar view, highlighting the necessity of information sharing. Deputy CEO of Customs, Mrs Marion Grant, informed the committee that intelligence sharing was key, stating:

> In our experience, the most successful outcomes are achieved when intelligence is shared between partners such as the Australian Crime Commission, the Australian Federal Police, counterpart state and territory police and crime commissions and particularly when we set up joint operational responses.[46]

3.66 Mr Richard Janeczko, a private security consultant with an extensive background in customs agencies, also noted the importance of targeting operations through the use of intelligence, stating:

> A lot of successful seizures of narcotics and tobacco, and other seizures, around Australia go down to very good intelligence, targeting and information sharing with other agencies.[47]

3.67 An example of this in practice was the October 2010 seizure of 464 kg of cocaine in Brisbane. Intelligence from the United States Drug Enforcement Administration, referred to Australian law enforcement agencies through the Australian Federal Police international network (discussed below), led to a successful, directed joint operation by the AFP and the Australian Customs and Border Protection

---

44 AFP, *Submission 19*, p. 7.

45 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, pp 38–39.

46 Mrs Marion Grant, Deputy Chief Executive Officer, Customs, *Committee Hansard*, 17 February 2011, p. 3.

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

Agency.[48] The committee considers that the interception of such an importation, using the small boat methodology, would have been unlikely in the absence of intelligence, as Mr Phelan noted in relation to that case:

> Of course one of the vulnerabilities, as we have seen with our major seizures this year, is that it does not always happen at the major seaports. It is coming through small craft that meet mother ships outside. That is the whole coastline. It is simply not practical to have people at every one of those and checking every pleasure craft that comes [in]. It is all about intelligence.[49]

3.68 The committee is firmly of the view that the continuing success of law enforcement operations combating serious and organised crime in the aviation and maritime sectors will require the timely and effective use of criminal intelligence. As noted by the agencies, the effective use of intelligence requires sharing and cooperation between law enforcement partners.

The importance of international intelligence

3.69 Serious and organised crime is increasingly a transnational affair, with criminal 'networks of opportunity' operating across international borders. A national response to organised crime therefore requires coordination with international partners. The importance of international cooperation is recognised in the Commonwealth Organised Crime Strategic Framework, which states:

> Given the growing geographical reach of organised crime and the increasing globalisation of financial markets, international cooperation and engagement is a vital part of dismantling organised criminal activities and networks.
>
> The successful understanding of, and intervention against, organised criminal activity, including prosecution, is dependent on effective frameworks for international cooperation. Particularly important are the tools of information and intelligence sharing and police to police assistance to build a comprehensive understanding of the networks. International cooperation, including through mutual assistance and extradition, will be critical to prevent perpetrators from evading sentencing, or concealing the proceeds of crime by crossing international borders. Dedicated and ongoing effort to improve the capacity of regional and developing countries is also integral to preventing and disrupting organised criminal activity before it reaches Australia's borders. The Commonwealth is responsible for

48 AFP, 'Drug syndicate smashed, 464kg of cocaine seized', Media release, http://www.afp.gov.au/media-centre/news/afp/2010/october/drug-syndicate-smashed-464kg-of-cocaine-seized.aspx (accessed 8 March 2011).

49 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 43.

> delivering international law enforcement cooperation and engagement and has developed a range of mechanisms for this purpose.[50]

3.70 From the evidence provided to the committee, the primary source of overseas criminal intelligence used to combat serious and organised crime appears to be the Australian Federal Police International Network.

3.71 The International Network consists of more than 85 AFP officers based in 30 countries. These AFP International Liaison Officers serve as the Australian Government's law enforcement representatives overseas.[51]

3.72 In addition to the international liaison officer network, the AFP submission also noted wider international engagement strategies by the agency, including capacity building projects such as the provision and training of foreign law enforcement agencies, operational deployments overseas and cooperation through involvement in international crime centres and multinational policing organisations.[52]

3.73 Through these functions, the AFP conducts enquiries on behalf of all Australian State, Territory and Federal law enforcement agencies and cooperates with other Australian Government departments domestically and abroad. This is intended to facilitate a 'whole-of-government' approach to fighting crime at its source.[53]

3.74 The AFPA noted the value of the AFP liaison network in particular, stating:

> [O]ur understanding from our members is that the AFP has a somewhat extraordinary international network that works extremely well with various countries. So, again, we have got the structure in place for dealing with trans-national crime and organised crime and terrorism.[54]

3.75 In addition to the AFP network, other agencies maintain their own links with overseas partner agencies and organisations. For example, Customs sources intelligence from the World Customs Organisation and its subsidiaries, and a long list of foreign customs and border protection agencies.[55] Similarly, many other agencies may have their own overseas partner agency sources.

---

50 Australian Government, Commonwealth Organised Crime Strategic Framework, p. 7.

51 AFP, 'International network', http://www.afp.gov.au/jobs/current-vacancies/international-liaison/international-liaison-information.aspx (accessed 12 April 2011).

52 AFP, *Submission 19*, p. 2.

53 AFP, 'International network', http://www.afp.gov.au/jobs/current-vacancies/international-liaison/international-liaison-information.aspx (accessed 12 April 2011).

54 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 37.

55 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

3.76 Intelligence and information sharing is also facilitated through international law enforcement organisations, most notably Interpol and Europol.[56]

3.77 The committee accordingly considers the AFP international network to be a valuable asset. It is therefore keen to ensure that the information obtained through the network continues to be used effectively in coordinating domestic law enforcement efforts.

Agency level sharing arrangements

3.78 As noted at the outset of this section on intelligence-led policing, the sharing of intelligence is critical to its effective use. For this reason, the committee would like to see enhancements to current intelligence sharing mechanisms.

3.79 There are several main institutional criminal intelligence sharing mechanisms within the Australian law enforcement community.

3.80 The ACC manages the Australian Criminal Intelligence Database (ACID and the Australian Law Enforcement Intelligence Network (ALEIN). ALEIN is a secure extranet that facilitates access to services including ACID. ACID itself allows federal, state and territory law enforcement and other regulatory authorities to securely store, retrieve, analyse and share criminal information and intelligence on a national basis.[57]

3.81 The ACC provided information to the committee about ACID and ALEIN, stating:

> ACID and ALEIN provide law enforcement with the tools to assist with identifying, analysing and sharing critical pieces of information including new criminal trends, emerging methodologies and links between criminal activities and criminal targets. The ACC draws on the criminal intelligence holdings in ACID to develop national criminal intelligence.[58]

3.82 Of particular interest for this inquiry is the dissemination of ACC information reports involving organised crime in the aviation and maritime sectors via ACID. As part of the special investigations conducted by the ACC into those sectors, over 500 individual information reports were uploaded to ACID for the use of federal and state law enforcement partners.[59]

---

56 Customs, answer to written question on notice , 9 May 2011 (received 25 May 2011).

57 Australian Crime Commission, 'ACID/ALEIN' http://www.crimecommission.gov.au/our_work/acid_alein.htm (accessed 13 April 2011).

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

59 ACC, *Submission 8*, pp 3–4.

3.83 The Australian Crime Commission also houses the Criminal Intelligence Fusion Centre, which was formally established in July 2010.[60] The Fusion Centre consists of collocated officers from key agencies including the Australian Taxation Office, the AFP and Centrelink to allow 'faster, more accurate and more effective exchange of intelligence between agencies.'[61]

3.84 The ACC informed the committee that officers in Fusion Centre work collaboratively to provide a more comprehensive picture of the targets, risks, threats and vulnerabilities associated with criminal activity, explaining:

> This means that the data can be fused in near real-time, the results analysed and fed back to agencies to act upon. The ACC believes that the fusion capability will have a strong response to, and impact on, serious and organised crime.[62]

3.85 A number of committees and other forums facilitate high level information sharing between law enforcement agencies. These include the ACC Board itself, made up of the heads of key Commonwealth agencies and state and territory police commissioners, the Australia New Zealand Policing Advisory Agency Crime Forum and the Serious and Organised Crime Coordination Committee.[63]

3.86 Additionally, the Heads of Commonwealth Operational Law Enforcement Agencies is the government's primary consultative mechanism for law enforcement issues and plays a role in discussing the outcomes of criminal intelligence.[64]

3.87 The Tripartite Operations Group acts as a management-level committee that provides ongoing liaison at a national level between the ACC, AFP and Customs in relation to operations and intelligence.[65]

3.88 The ACC also informed the committee that law enforcement agencies regularly liaised on a bilateral basis, facilitating the sharing of intelligence.[66]

3.89 In its submission to the inquiry, Customs described its liaison officer network, through which it maintained communication with other state and federal law enforcement and regulatory agencies. Customs informed the committee that in the 12

---

60 ACC, 'Fusion Centre', http://www.crimecommission.gov.au/media/faq/fusion.htm (accessed 13 April 2010).

61 The Hon. Brendan O'Connor MP and the Hon. Robert McClelland MP, 'Additional $38.5 million to Combat Serious and Organised Crime', *Joint Media Release*, 11 May 2010.

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

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

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

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

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

months prior to November 2009, strong results had been achieved as a result of cross-agency communication and interaction through the liaison officer network.[67]

3.90 Customs also noted that intelligence was shared on a number of levels, under the umbrella of Memoranda of Understanding (MOUs), subject to requirements of the *Customs Administration Act 1985*.[68]

3.91 The committee received some information about the growing relationship between national security agencies and the law enforcement community. The ACC noted that the Australian Intelligence Community provides to it national security intelligence on an as-needs basis and vice versa.[69]

3.92 Since the then Prime Minister's inaugural National Security Statement in 2008, an expanded national intelligence community had been created to reflect changed global, strategic and threat environments, including serious and organised crime. At its broadest level, this effort is coordinated by the National Intelligence Coordination Committee (NICC). The NICC consists of all national intelligence, security and law enforcement agencies and is the most senior mechanism for whole-of-government strategic coordination of national intelligence.[70]

3.93 The committee was not able to fully explore the state of information sharing mechanisms between Commonwealth, state and territory agencies, however it did receive mixed evidence on the subject. The Western Australian Police, submitted that the provision of intelligence from federal to state agencies was cumbersome, explaining:

> Interoperability between State and Federal law enforcement agencies in Western Australia is adequate with intelligence and technical sharing available on a consistent basis. Of recent times, diminished resources on the part of the ACC and AFP in Western Australia has left WAPOL in a better position to contribute human resources. The process of intelligence sharing from State to Federal remains simple and unhindered by process.
>
> In reverse, however, the flow of intelligence remains cumbersome and administratively slow. On occasions, the processes involved are an impediment to dynamic and spontaneous operational environments. The ACC Act does enable direct dissemination under critical circumstances but these provisions are rarely utilised. All agencies operate intelligence databases in isolation, uploading to ACID and ALEIN as central databases... A streamlined, accountable process of accessing National

67 Customs, *Submission 13*, p. 11.

68 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

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

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

> intelligence holdings would further benefit frontline serious and organised crime investigators.[71]

3.94 Victoria Police also noted that there was scope for improvement in intelligence sharing mechanisms, submitting:

> Intelligence is vital to informing decisions with respect to response options to organised crime in Australia's airports and port. Improvements can be made in relevant agencies' capacity and capability to collect timely and relevant intelligence with respect to airports and ports. This would include greater collaboration, interoperability between intelligence systems (where appropriate), better coordination of resources against agreed priorities, broadening the scope of intelligence and information collection and enhancing analytical capability.[72]

3.95 The committee encourages agencies at the state and Commonwealth levels to continue to develop information sharing capability.

3.96 In addition to agency level sharing mechanisms, there are a number of established taskforces or joint intelligence operations based around specific crime types, targets, environments or criminal methodologies. The next section describes how these taskforce approaches have been applied specifically in the aviation and maritime sectors.

Sectoral sharing arrangements

3.97 Earlier in this chapter, the committee described the need for permanent taskforce approaches to the coordination of law enforcement activity in the aviation and maritime sectors. These same structures can be, and are used to improve the flow of information and intelligence between officers working within those sectors.

3.98 At airports, the JAIG model, supplemented by JAITs, brings together officers of the key law enforcement agencies in order to collaborate on the collection and sharing of relevant intelligence. As noted above, this appears to have been relatively successful.

3.99 Within the port environment, various taskforces have been established including the NSW Port Crime Taskforce, also described above. The committee has also observed, during site visits, close cooperation between state and Commonwealth officers, resulting in successful operations.

3.100 The degree to which such arrangements succeed appears to the committee to rely on the establishment of a positive, information sharing culture. This varied across the jurisdictions visited by the committee. For this reason, the committee reiterates

---

71 Western Australia Police, *Submission 3*, pp 2–3.

72 Victoria Police, *Submission 10*, p. 2.

recommendations above that more permanent maritime taskforce arrangements be established in each state and territory.

3.101 The establishment of the NSW Port Crime Task Force is an example of how agencies can enhance collaboration, and follows other successful joint-agency special investigations. Continual improvement of agency cooperation and information sharing will no doubt be required to keep pace with developments in organised crime networks. Given the international nature of organised crime, the need for law enforcement cooperation is likely to extend to overseas counterparts.

Continual improvement of strategic and tactical use of intelligence

3.102 Information, particularly intelligence, is a precious commodity in the law enforcement environment. For this reason, the committee strongly encourages the law enforcement community to continue to improve the flow of information between agencies.

3.103 The committee is pleased to observe that information sharing does appear to have improved, particularly over the last two years. The implementation of the committee's recommendation to establish taskforce models in each state and at the national level will ensure that tactical use of intelligence is maximised by teams working within each sector. Intelligence-led operations are effective and efficient and are strongly supported by the committee.

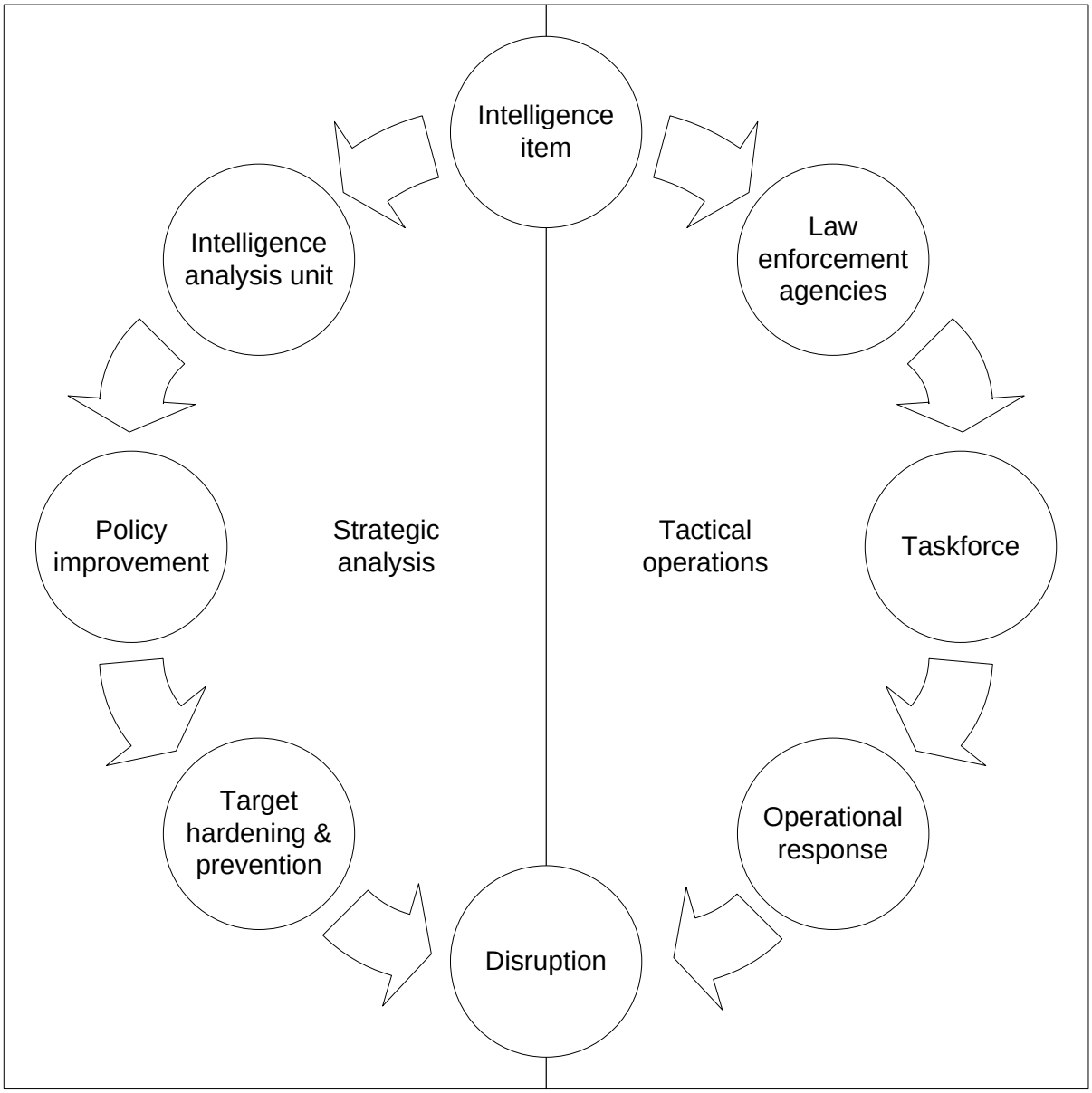
3.104 It is important to also improve upon the strategic use of intelligence, by continuing to build a picture of criminality that can be used to remove future criminal opportunities. Mr Phelan noted the importance of the strategic approach, stating:

> While Australia's air and sea ports remain vulnerable to infiltration by organised crime, especially for the import and export of illegal goods and proceeds of crime, our national responses to organised crime need to remain holistic and open-minded. A strategic response to organised crime will naturally incorporate links to the broader environment, including potentially all sea and air ports, but must remain conscious of the wider networks and implications both domestically and internationally.[73]

3.105 The strategic and tactical uses of intelligence are depicted in figure 3.1, which indicates how both approaches seek to disrupt criminal activity.

73 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p. 38.

Figure 3.1: The two-track use of received intelligence



3.106 In the context of aviation and maritime security, the broad contours of both approaches are already in place. On the tactical side, dedicated taskforces in the aviation sector, and gradually developing taskforces in the maritime sector, are bringing together the intelligence and information held by individual agencies. Strategic analysis is undertaken by the ACC, with reports provided to law enforcement partners and policy groups.

3.107 The ACC identified a number of areas for future enhancement of information sharing. These included:

- the need to develop consistency across Australia in the collection, analysis and exchange of intelligence;

- opportunities for the improved use of ACID and ALEIN;
- continued development of the criminal intelligence fusion capability; and
- further improving the timely exchange of information between both law enforcement and national security agencies.[74]

3.108 The committee encourages the law enforcement community to continue to remove barriers, whether cultural or organisational, in order to enable the appropriate flow of information for both strategic and tactical purposes.

Private sector involvement

3.109 Successfully combating the threat of serious and organised crime in the aviation and maritime sectors will require the engagement and involvement of the private sector groups operating in those environments.

3.110 A large amount of information that could be used by law enforcement agencies is held by private sector organisations including passenger details, cargo manifests and employment records. Much of this information is properly subject to privacy laws and other protections. Nevertheless, within these constraints, the continual development of a good relationship between law enforcement agencies and private organisations is valuable.

3.111 One of the main areas where this issue arose was in the provision of passenger information by airlines. Given the importance to law enforcement agencies of the ability to track the movement of 'persons of interest', airlines are subject to a number of requests for such information each year. Mr Stephen Jackson, Qantas, explained that unlike some other industries, it was Qantas to policy to provide such information free of charge, stating:

> In any one year, on average we service law enforcement inquiries up to the number of 6,000. We do not charge for those. The example was given in relation to the telecommunications industry. My knowledge of interaction with Telstra in the sense of information for court record analysis six or seven years ago is that it was $35 an inquiry. Last night my security controller on duty spent 70 per cent of his shift dealing with law enforcement inquiries.[75]

3.112 Mr Jackson informed the committee that Qantas sought to comply with such requests to the best of their ability, commenting:

> In terms of the generic answer, as long as we operate within the bounds of the law in terms of our compliance with privacy legislation and the agencies comply with their own respective secrecy provisions, my instruction to my

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

75 Mr Stephen Jackson, Qantas, *Committee Hansard*, 18 February 2011, p. 28.

> staff is that they are to provide full and unfettered access to whatever information is requested.[76]

3.113 However, the committee also understands that the timely provision of such information often relied on the relationship an agency could build with a private company. The committee notes that many of the private organisations that provided evidence desired a closer relationship with law enforcement agencies in order to deliver better and more informed company security policies. For example, Qantas made the following comment:

> To enable the aviation sector in partnership with law enforcement agencies to effectively counter current and next generation criminal threats, it is critical that an information and intelligence sharing system is embedded that ensures the flow of timely and accurate information between parties. Such information would enable Qantas to more effectively identify vulnerabilities that may be subject to exploitation now or in the future... The precedent already exists in the national security environment, where the rapid sharing of that information enables Qantas to react in advance to any identified threat issues.[77]

3.114 As Mr Michael Carmody observed, current information sharing arrangements are ad-hoc and could benefit from a formal framework that involved database access of some description, stating:

> Yes, airlines, particularly, do maintain connections with other airlines and, in some cases, other governments with regard to high-profile threat so that, if someone is identified boarding a Qantas aircraft in London, that name may trigger if those connections are in place. Fundamentally, though, we have no framework in place to react to this. It really is reliant at the lower level on the airline network to plug in mate-to-mate, for want of a better term, to try to access certain data and pull it in. It is a very rough system when you consider that one mistake at that screening point could cause the deaths of 400 people.[78]

3.115 There are no doubt barriers to the sharing of information between law enforcement agencies and the private sector. For example, from a purely logistical perspective, CrimTrac noted that its current operating mandate did not extend to non-government bodies. Mr Douglas Smith, CrimTrac, stated:

> The mandate that is given to CrimTrac comes from an intergovernmental agreement which was first signed back in 2000. That is, if you like, the contract that brings together the various jurisdictions. The short answer to your question is that we have no mandate to deal with private companies. If we were to deal with private companies in providing that sort of capability,

---

76 Mr Stephen Jackson, Qantas, *Committee Hansard*, 18 February 2011, p. 34.

77 Qantas, *Submission 5 (supplementary)*, p. 6.

78 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 4.

there are a whole raft of privacy, legislative and other practical issues that would have to be negotiated.[79]

3.116 The issue of information sharing is again raised in the context of passenger profiling in Chapter 4 and ASIC and MSIC cardholder information held by AusCheck, discussed in Chapter 5.

3.117 The committee has had the opportunity to discuss the issue of private sector and law enforcement agency cooperation in detail during site visits around Australia. The committee is accordingly convinced of the need to improve the information sharing relationship to both aid law enforcement investigations and allow private organisations to play an enhanced role in security.

3.118 Such an initiative could build on the existing Trusted Information Sharing Network (TISN) which provides an environment where business and government can share vital information on national security issues relevant to the protection of critical infrastructure and the continuity of essential services in the face of 'all hazards'.[80]

3.119 The TISN supports the Australian Government's Critical Infrastructure Resilience Strategy, which aims to support the continued operation of infrastructure critical to Australia's national defence and national security. As such, the TISN has a different purpose to the information sharing arrangements desired by the committee. It therefore recommends that the Attorney-General's Department develop a possible model for the enhanced provision of information between public and private entities for the purpose of strengthening the response to serious and organised crime.

Recommendation 5

3.120 The committee recommends that the Attorney-General's Department conduct a review of current information sharing arrangements between law enforcement agencies and private organisations in the aviation and maritime sectors.

79 Mr Douglas Smith, CrimTrac, *Committee Hansard*, 18 February 2011, p. 48.

80 Attorney-General's Department, 'Critical Infrastructure Resilience', http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection?open&query=TISN (accessed 21 April 2011).

Chapter 4

'Hardening' the environment

Introduction

4.1 While the previous chapter dealt with the law enforcement response to serious and organised crime, this chapter deals with specific security measures within the aviation and maritime sectors. This includes physical security and other measures which reduce the vulnerability of the sectors to exploitation by serious and organised crime.

4.2 The process by which a particular environment is secured against criminal exploitation is referred to as 'hardening'. In essence, these measures make it harder for criminals to operate, in this case, within the aviation and maritime sectors.

4.3 In addition to the public evidence provided to the committee through submissions and at public hearings, the committee has also visited airports and seaports around Australia. These visits, including discussion with government officials and private employees, have allowed the committee to make comparisons between the security regimes of each facility.

4.4 The committee's findings are split between the aviation and maritime sectors. Issues relating to the aviation sector include passenger identification and screening, the commercialisation of airports, and security outside of the major airports. Issues in the maritime sector include uneven security arrangements between ports, container inspection and access to the port precinct. The potential to further improve CCTV is relevant to both the aviation and maritime sectors and is discussed in the context of both.

Issues in the aviation sector

Securing the aviation passenger stream

4.5 A range of issues were raised with committee with regards the security of the aviation passenger stream. These issues particularly related to the verification of identity of passengers, which could facilitate the appropriate monitoring of persons of interest, the matching of appropriate security measures to individual passenger risk and the treatment of access to sterile areas in airports. These issues are addressed below.

Passenger identity

4.6 Currently, domestic air passengers are not required to show photo identification in order to check-in and board an aircraft. Specifically, there is no legal requirement to do so.[1]

4.7 The Western Australia Police presented evidence to the committee that individuals involved in serious and organised crime were regularly travelling under assumed identities in order to evade police detection.

4.8 Ms Maggie Plumb presented research using WA Police information that documented a number of such cases. Ms Plumb's research identified four separate cases, involving 13 offenders who were known to have used false travel names to facilitate criminal activity.[2] These cases involved the distribution of significant quantities of illicit drugs and money laundering. Ms Plumb noted that the ability to travel under a false identity created a significant loophole undermining other airport security measures:

> Screening is a really important issue at airports. It is taken very seriously at international airports, but we seem to have a practice at domestic airports of being very trusting and believing that everybody is doing the right thing. However, we know that is not the case. Screening at the airport entails security staff and CCTV networks; airport staff are screened and display their ASIC; there are other metal detectors and bomb residue screening of passengers; there are canine patrols who search for food, explosives, drugs and currency; but nobody is screening for passenger identity.[3]

4.9 Ms Plumb also identified as a problem the difficulty the use of false identities caused investigators, stating:

> With regard to policing—and this affects not just WA police—passengers who fly on domestic aircraft under false names create barriers to many investigations, including serious and organised crime, gang crime, major fraud, major crime, missing persons and disaster victim identification.[4]

4.10 These concerns were shared by Mr Michael Carmody, who had previously served as the Head of Security at the former Federal Airports Corporation, who observed:

> The other crazy thing we have is that not only within our regional airports but even within our domestic airports we allow people to enter the sterile area who are not passengers. It creates a significant concern. Do you realise you can board a domestic aircraft today and never show your identification to anyone? You can put yourself on an aircraft this afternoon, a 767,

1 Qantas, *Submission 5 (Supplementary)*, p. 5.

2 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 5.

3 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 4.

4 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 4.

> capable of flying anywhere, and no-one verifies either your identification or verifies you to the ticket to the bag. And when you enter the sterile area, because there are non-flying persons in that sterile area, you can swap your ticket with anyone and that person could then board the aircraft.[5]

4.11 Western Australia Police informed the committee that the ability to travel under a false identity, combined with the lack of a formal passenger alert system as exists in the international setting, made it difficult to adequately investigate the movement of persons of interest. Detective Superintendent Charles Carver stated:

> With investigations in relation to serious and organised crime, with international flights you have the ability to put PACE alerts on. Basically you are advising that these people are at the airport or are flying on this particular plane. There are provisions there for it to be checked off as they come through; they check in and they are on the manifest. We do not have a domestic PACE alert, so in a serious and organised crime investigation it is very difficult for us and the states and territories to get in front of the play. Firstly, if they are using false identification, they could still use false identification even under a new regime, but the thing is that, if we have PACE alerts and we know they are using those false names and we have access to those manifests, it makes it very much easier to get in front of the play as far as investigations are concerned.[6]

4.12 Det. Supt Carver expressed concerns that the ease with which domestic air travel could be used to distribute drugs to WA contributed to that state's drug problem, stating:

> Because of our vibrant economy in Western Australia we are a target for these organised criminal syndicates, gangs and groups to traffic their drugs across to this state, and we pay top dollar for it. The reason we are so concerned about the aviation industry is that those drugs are coming through on the domestic side. That is why we are here today—to bring our concerns to the table and to say that that is fuelling the drug problem in this state.[7]

4.13 As a result of her research, Ms Plumb recommended the introduction of Commonwealth legislation that would require domestic airline passengers to authenticate their identity.[8]

4.14 The Australian Federal Police Federation was also in favour of the creation of such an offence, stating:

> We can understand the commercial imperatives that may be there with regard to the airlines saying they want to use the automatic ticketing system

---

5 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 6.

6 Det. Supt Charles Carver, WA Police, *Committee Hansard*, 10 November 2010, p. 9.

7 Det. Supt Charles Carver, WA Police, *Committee Hansard*, 10 November 2010, p. 13.

8 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 8.

> or, indeed, online booking. But what we would like to see is that there is a specific offence in play for the situation where someone travels on false identification. This becomes very important in relation to future investigations by law enforcement agencies, including the Australian Federal Police, where we may identify criminals who have travelled on false bookings—and, of course, there is no defence for that—and that might be part of an investigation of proving continuity in an offence et cetera. It is beneficial to have an offence.[9]

4.15 The AFPA noted that such a measure may have to include certain provisions to ensure that it did not result in unintended consequences. This included the need for a 'reasonable excuse' clause. Mr Jonathan Hunt-Sharman explained that in their proposal:

> Importantly, we have reasonable excuse built in. This is not about people making an error or people trying to avoid—where, for personal circumstances, they are trying to get on a flight to leave a state without someone knowing. If there is a reasonable excuse for the behaviour, then it would be looked at...[10]

4.16 The committee agrees that the ability to travel under a false identity is significant enough to warrant the creation of a new offence. The committee therefore recommends that it be made an offence to deliberately travel under a false name on a domestic aircraft.

Recommendation 6

4.17 The committee recommends that the *Crimes (Aviation) Act 1991* be amended so as to create a new offence of deliberately travelling under a false identity.

4.18 Ms Plumb also recommended that passengers be required to verify their identity at the point of check-in to further ensure that individuals could not travel under a false identity.[11]

4.19 The Australian Service Union expressed a similar sentiment, noting the importance of interaction between customer service staff and passengers to security, stating:

> In an effort to cut labour costs airlines have increasingly been replacing staff with electronic check in machines which allow passengers to simply enter a reservation or frequent flyer number and receive their boarding pass. They are not required to show identification and need have no contact with a Customer Service Agent. This removes an important layer of security

9 Mr Jonathan Hunt-Sharman, Australian Federal Police Association, *Committee Hansard*, 17 February 2011, p. 29.

10 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 29.

11 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 10.

> where Customer Service Agents at check in assess the demeanour of the passenger and most critically check their identity.[12]

4.20 Such a move would potentially affect the ability to use electronic check-in processes.

4.21 Qantas did not support the introduction of identity checks for domestic airline passengers. It was against such a measure given the difficulties of establishing a sufficiently robust system of identification assessment, stating:

> As the Committee is aware, there is currently no Commonwealth legislation that requires verification of passenger identity prior to uplifting a passenger on domestic airline services. Nor is there any common form of identity document available to Australian nationals that could be used to meet any such requirement, presenting problems for particular categories of persons including unaccompanied minors, infants, people without driver's licenses, passports or any other form of photographic identification.[13]

4.22 According to Mr Stephen Jackson, Qantas, this last category included many elderly passengers who had never held identity documents. Mr Jackson also argued against the introduction of identity checks on the basis that airline employees were not trained to recognise fraudulent documents.[14]

4.23 Finally, Qantas also opposed the introduction of identity checks on the basis of the cost of introducing a sufficiently robust system estimating the cost to be 'many millions of dollars, not including data storage and transmission costs.'[15]

4.24 From the evidence provided, including the committee's own observations during inspection tours at major Australian airports, the committee is concerned that that the e-ticketing process introduces further vulnerabilities, increasing the opportunity for organised criminal networks to exploit the sector for illicit gain.

4.25 The committee is therefore recommends that the passenger's identity be checked at the point of embarkation, at the gate lounge. This would require passengers to display valid photo-identification that matched the name printed on their boarding pass immediately prior to boarding the plane.

4.26 The committee is of the view that this identity check should be undertaken by a government official, ideally a government security officer as provided for in recommendation 2. Such a scheme would also require a mechanism by which passengers that do not have identification can still travel on an aircraft. This could be

---

12 Australian Services Union, *Submission 7*, p. 8.

13 Qantas, *Submission 5 (Supplementary)*, pp 5–6.

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

15 Qantas, *Submission 5 (Supplementary)*, p. 6.

facilitated through the ability to provide a signed, statutory declaration confirming a passenger's identity.

Recommendation 7

4.27 The committee recommends that it be made a legal requirement to provide photo identification confirming passenger identity immediately prior to boarding an aircraft.

4.28 The committee recognises that there are a number of issues associated with identity and proof of identification. These include the forgery of photo identification and the ability of screening officers to properly assess identification documents.

4.29 A further issue relates to the ability of an individual to officially change their name. This practice can cause problems for the administration of criminal histories. As Det. Supt. Carver noted in relation to the process by which names are changed:

> Different regimes, different states, different territories, different ways of doing things. Again, it comes down to the states and territories getting their act together to look at the serious effect these offences have right across Australia—in fact, around the world.[16]

4.30 Change of name procedures are managed by the states and territories. This has led to a diversity of approaches by jurisdictions to change of name processes and the exchange of change of name information with law enforcement agencies.[17]

4.31 Attorneys-General around Australia have agreed to develop best practice change of name processes through a Standing Committee of Attorneys-General (SCAG) working group, led by NSW, which is intended to have concluded its work by the end of 2011.[18]

4.32 The committee considers that this and other issues relating to identity and identification are of serious concern. As a result, the committee may conduct an inquiry into issues of identity and law enforcement.

Passenger profiling

4.33 An issue closely related to the accurate verification of identity is the ability to build individual risk assessments around passenger information. Mr Michael Carmody argued in favour of the use of passenger profiling, stating:

> It is not the point of the aviation protective measure to stop the chap in the eleventh hour of the process. You have to start the issue of aviation security

16 Det. Supt Charles Carver, WA Police, *Committee Hansard*, 10 November 2010, p. 22.

17 Senator the Hon. Joe Ludwig, Minister for Agriculture, Fisheries and Forestry, Questions without notice: additional answers, *Senate Hansard*, 12 May 2011, p. 54.

18 Senator the Hon. Joe Ludwig, Minister for Agriculture, Fisheries and Forestry, Questions without notice: additional answers, *Senate Hansard*, 12 May 2011, p. 54.

> and the application of protective measures right from the point of ticket purchase. You do this by applying what is loosely termed 'passenger profiling'.[19]

4.34 Customs already adopts a profiling approach to incoming international passengers and aircrew, as outlined in its submission:

> Customs and Border Protection contributes to delivering aviation security, including the identification of criminal activity, through the profiling of passengers and crew. A number of systems are used to analyse flights to Australia and assess passengers and crew prior to their arrival. This analysis enables the deployment of our intelligence, targeting, inspection, examination, detection and investigation capabilities to reduce and target the movement of persons or goods of terrorist or criminal concern.[20]

4.35 Mr Carmody outlined the potential of passenger profiling by reference to the use of software within Israel. Passenger information, including the manner in which a ticket is booked through to personal details are assessed using software right from the point of ticket sale onwards. The information is used to build a risk profile for each individual, which can then affect the level of security applied to that individual upon arrival at the airport, such as further questioning at check-in.[21]

> This process of analysing the profile continues all the way through, inclusive of [check-in]. At [check-in], once you put your bag on that counter the screen lights up, the name is there and the check-in assistant already understands where you sit in the profiling technique. There is a series of Q and A to confirm certain aspects of that if appropriate, and if you fail the profiling point at that stage there is normally someone who will ask you to go with them. Your identification and verification of flight details will be checked. The point of the exercise in profiling is, in a risk management sense, to highlight and identify your most serious risk before they hit the screening point, let alone the aircraft. We tend to engineer it in reverse; we tend to hope that at the eleventh hour we catch someone walking through a screening point or, better still, stumble across something as they mount the aircraft and sit in a seat.[22]

4.36 Mr Carmody informed the committee that the primary consideration in the establishment of such a scheme was the ability to share information. He noted:

> Yes, airlines, particularly, do maintain connections with other airlines and, in some cases, other governments with regard to high-profile threat so that, if someone is identified boarding a Qantas aircraft in London, that name may trigger if those connections are in place. Fundamentally, though, we have no framework in place to react to this. It really is reliant at the lower

---

19 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 3.

20 Customs, *Submission 13*, p. 8.

21 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 3.

22 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 3.

> level on the airline network to plug in mate-to-mate, for want of a better term, to try to access certain data and pull it in. It is a very rough system when you consider that one mistake at that screening point could cause the deaths of 400 people.[23]

4.37 Mr Kim Langton, Chameleon Associates (Australia) also supported the introduction of domestic passenger profiling, emphasising the importance of the human side of security, stating:

> You have to remember with technology—and I think our reliance on technology is far too great; we ought to bring back the human element—if there is an X-ray machine that they are using at the airports and you are dealing with state sponsored terrorists who have a lot of money, what is to stop them from buying that same machine, pulling it apart, working out what works and what does not work and then setting their plan to it? The only thing they cannot count on is a security guard coming up to them and asking them a question, because they do not know what they are going to get asked. That is where profiling and questioning come into it.[24]

4.38 Qantas agreed that in a layered approach to aviation security, passenger profiling had merit, but that it had not been tested within the Australian domestic aviation environment. Qantas did note that any passenger profiling would necessarily be the responsibility of suitably trained government authorities.[25]

4.39 As a secondary consideration to passenger profiling, Qantas did note that it supported the presence of officers from government agencies at check-in or screening points. Qantas argued that this would considerably enhance the deterrence factor against those engaging in criminal (and terrorist) activity, while providing opportunity to conduct behavioural analysis of passengers.[26]

4.40 The committee agrees that passenger profiling would significantly enhance aviation security from both a counterterrorism and organised crime perspective. However, it is mindful of some of the difficulties inherent in sharing information between private and public entities. As Qantas noted in its supplementary submission:

> In relation to the release of passenger information, Qantas is bound not only by Commonwealth Privacy legislation, but by European Union Privacy legislation. Passenger information is collected and stored in the Amadeus Reservation System which is "warehoused" in Europe – as such Qantas is obligated to comply with European Union legislative requirements.[27]

---

23 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 4.

24 Mr Kim Langton, Chameleon Associates (Australia), *Committee Hansard*, 18 February 2011, p. 59.

25 Qantas, *Submission 5 (Supplementary)*, p. 6.

26 Qantas, *Submission 5 (Supplementary)*, p. 6.

27 Qantas, *Submission 5 (Supplementary)*, p. 9.

4.41 In addition, Qantas also noted the difficulties posed by airline reservation systems, which are not intelligence databases and therefore do not have a name matching capability, making name searches time consuming and resource intensive.[28]

4.42 The committee therefore recommends that the Commonwealth Government conducts further research into developing a system for the sharing of information held by airlines and air cargo agents with law enforcement agencies, and particularly the ACC Fusion Centre. The committee considers that the information would be most benefit if provided to the Fusion Centre, given its multi-agency approach to intelligence collection and analysis.

4.43 This research should include technical solutions that would enable 'live' access to data, the likely costs of such a system and the implications for statutory or other barriers to the sharing of such information. This research could possibly be conducted together with the broader review of public and private sector cooperation recommended in Chapter 3.

Recommendation 8

4.44 The committee recommends that the Commonwealth Government review the technical and administrative requirements necessary to facilitate the effective sharing of information between airlines and air cargo agents and law enforcement agencies and the Australian Crime Commission Fusion Centre for the purpose of enhancing aviation security and law enforcement activities. The review should include research into technical requirements for such a scheme, the costs involved and any relevant statutory or other barrier to the sharing of such information. The findings of the review should be reported to the Australian Parliament.

Restricting access to the sterile area

4.45 During inspection tours at airports, the committee was able to closely examine the screening mechanism in place between the public access area of the airport and the 'sterile' area, within which all individuals are expected to have been screened for weapons and other dangerous items. In general, the integrity of these screening measures and the sterile area is enhanced by reducing the number of people entering the area.

4.46 The committee heard from a number of witnesses that the growth in commercial outlets within the sterile area, had inflated the number of people passing through screening points, to the possible detriment of security outcomes.

4.47 Combined with the free access of non-travelling members of the public, this put excessive pressure on screening point. This is contrast to international air travel or domestic travel in certain other countries, where access is restricted to passengers and

28 Qantas, *Submission 5 (Supplementary)*, p. 9.

those with a business reason to enter the area (for example employees and government officials). For example, the United States of America does not permit non-flying members of the public to enter the sterile area, reducing the number of people passing through screening points.[29]

4.48 The development of airports as commercial hubs has increased the natural tension between commerce and security in that sector. The advent of airport shopping centres and other new commercial interests has increased the number of people on site both as employees and customers. Airports, with a focus on the movement of passengers, also must contend with far greater public access to facilities as compared to ports that are primarily concerned with cargo. Mr Michael Carmody, former Head of Security for the Federal Airports Corporation, was of the opinion that airport design focused on commercial interests first and security issues second.[30]

4.49 Ms Linda White, ASU, commented on the increasing focus on retail within the sterile airport environment, stating:

> The more people that you have that you have to screen, the more pressure it puts on the system, the more people have to be watched, the greater the turnover there may well be—and, to us, this is an airport, where the primary focus is flying and the transport of cargo and passengers. It is not about retail. The passenger experience—while we understand this—is where airports make their money. But, if you are focusing on the people who work for airlines and airports because they have this access, we say: why don't you limit the number of people who can be there?[31]

4.50 The committee notes that in addition to more people in the screening area, the stocking of retail outlets would also result in a high flow of goods into the restricted area, with a commensurate potential for smuggling.

4.51 The ACC also commented on the challenge to security posed by the increasing commercial development of secure areas within the airport. Mrs Kathleen Florian informed the committee that:

> I think that poses significant challenges from a number of points of view. I suppose some of the issues that it raises are the increasing commercialisation of shopping precincts within airport infrastructure; the moving of international flights from CTFR airports into some regional airports has created issues. The nature of some flights that go from those airports to key destinations, particularly in South-East Asia, may be significant from an illicit commodity sourcing point of view. Some of those commercial issues certainly do raise questions about serious and organised

---

29 Unites States Department of Homeland Security, Transport Security Administration, 'ID Requirements for Airport Checkpoints', http://www.tsa.gov/travelers/airtravel/acceptable_documents.shtm (accessed 17 May 2011).

30 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 5.

31 Ms Linda White, ASU, *Committee Hansard*, 17 February 2010, p. 12.

crime within the airport and how to most effectively harden that environment.[32]

4.52 Mr Richard Janeczko was of a similar opinion, stating:

On the other question, the more people you have in an airport and the more traffic you have coming and going the more risk there has to be anyway because you have a larger number of people coming in and a larger number of people to check. There are legitimate goods that have to be in an airport. There are only a small percentage of those things you can target. The advantage of duty-free is probably a thing. We had a major success a year or two ago in uncovering and prosecuting people who ended up with five or six years in jail because they were getting around the duty-free laws. So greater commercialisation, in the sense that if you get a concession by buying at an airport that you could not get if you were not buying at an airport, has brought greater risks. Where there is a vulnerability you will find crime. I think the fact that it is a shopping centre where planes land has created a lot of opportunity.[33]

4.53 Finally, Mr Michael Carmody observed much the same point, stating:

That is all it is; everything is a cost issue. You have the airlines who are trying to drive passenger facilitation. From the time you pull into the carport to the time you put yourself on the seat, they want to get you through that process as quickly as they possibly can. Things like security and the checking and screening et cetera are limitations of that facilitation process. Airlines have a vested interest to get you on that aircraft and moving as quickly as they possibly can, so anything that gets in the way of that process is money. Over the years airport operators have turned an airport essentially into a shopping centre in which you park cars.[34]

4.54 Mr John McArdle, Australian Airport Association, did not see the existence of commercial outlets within the sterile areas as being cause for concern, stating:

The community that is travelling particularly in Australia expects certain 'pleasures' to detract them from the onerous task of waiting for aircraft or waiting for the processing that goes on. Retail is one of those measures that detract from the boredom of travel. I find it difficult to comprehend why anyone would say that retail is a threat within a terminal; be it in the Customs [area] or in the public area.[35]

32 Mrs Kathleen Florian, ACC, *Committee Hansard*, 17 February 2011, p. 11.

33 Mr Richard Janeczko, *Committee Hansard*, 17 February 2011, p. 19.

34 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, pp 4–5.

35 Mr John McArdle, Australian Airports Association, *Committee Hansard*, 17 February 2010, p. 1.

Airport design

4.55 Another issue is the difficulty inherent in retrofitting older airports with new security measures. Most of Australia's airports are decades old and as a result, are not designed to incorporate modern security concerns and technology. Sydney Airport Corporation Limited noted that newer airports overseas, such as Beijing, were built from green-field sites and hence were designed to take into account modern security concerns.[36]

4.56 This point was echoed by Mr Michael Carmody, who stated:

> If you take Sydney airport as an example, we started off in the very old Qantas terminal here 35 years ago, when you used to have that outdoor ground surveillance exercise and you walked to the aircraft et cetera. We then migrated across to what is now known as the international terminal—one pier. It has now generated the two pier and they are trying to build a third. Everything is fundamentally tacked on. Apart from providing adequate space to park an aircraft and the appropriate logistics to connect that aircraft, the rest is essentially around building a shopping centre. Anything that gets in the way of that process, particularly security, is an afterthought—'We will bang it in here.' If you have a look at any screening point, it is always at the narrowest neck, poorly laid out and poorly defined. Because the equipment is mobile, they set up a few barriers and dump the equipment in. And yet, conversely, with respect to Customs and AQIS, it tends to be built around those functions.[37]

4.57 The older design of most Australian airports is therefore a potential vulnerability. Based on the committee's inspection of various airports, newer terminals appear to incorporate modern security requirements effectively. In the absence of redevelopment of existing terminals, to the extent possible, retrofitting appears to be the only viable solution.

The use of sniffer dogs to deter drug smuggling and money laundering

4.58 During visits to airports and ports, the committee had the opportunity to assess the effectiveness of sniffer dog squads. The AFP trains and maintains an extensive detector dog capability, including the training of handlers and dogs that operate at Australian major airports. Firearms and Explosives Detector dogs are located at 10 major airports around Australia.[38]

4.59 Additionally, AFP sniffer dogs can also be trained to detect currency and illicit drugs. The Western Australia Police expressed a preference for more canine

---

36 Mr Grant Woods, Sydney Airport Corporation Ltd., *Committee Hansard*, 18 February 2010, p. 16.

37 Mr Michael Carmody, *Committee Hansard*, 18 February 2010, p. 6.

38 AFP, 'National Canine Capability' http://www.afp.gov.au/policing/aviation/canine-capability.aspx (accessed 10 May 2011).

squads at airports, with a view to detecting both drug trafficking and money laundering. Det. Supt Carver informed the committee that:

> I have put in submissions to put some operations in place and target specifically planes coming from Sydney and Melbourne, and leaving Perth to go to those particular locations, with drug dogs and also money dogs so that we can randomly intercept and basically distract and dismantle some of the activities that are going through the airports.[39]

4.60 Ms Maggie Plumb noted the use of sniffer dogs could serve two purposes. If unadvertised and randomised, the potential for actual interception was increased. Alternately, high profile, advertised searches would be unlikely to catch forewarned criminals, but might have a greater deterrent effect by virtue of the publicity.[40]

4.61 The committee supports the increased use of canine detection squads and is encouraged by the Commonwealth Government's decision to fund an additional 17 teams to operate at Australian airports by June 2011.[41]

4.62 The committee considers that the randomised and unadvertised use of currency and illicit drug detection dogs is of particular importance to combating serious and organised crime at airports. It therefore supports a further investment in these squads.

Recommendation 9

4.63 The committee recommends that the Australian Government provide further resources to support an increased presence for currency and illicit drug detection canine units at Australian airports.

Small aircraft movement

4.64 In addition to visiting major domestic airports in capital cities, the committee also visited General Aviation airports, including Jandakot Airport in Perth. The use of small non-commercial aircraft to facilitate the domestic distribution of drugs and other illicit goods has been publically documented. For example, in 2008, police intercepted 22 kilograms of methylamphetamine and 35 000 ecstasy tablets that had been brought to Jandakot Airport by light plane.[42]

4.65 The committee was therefore interested to examine the monitoring of small aircraft, which could potentially be used to import illicit substances from nearby countries including Indonesia and Papua New Guinea.

---

39 Det. Supt Charles Carver, WA Police, *Committee Hansard*, 10 November 2010, p. 19.

40 Ms Maggie Plumb, *Committee Hansard*, 10 November 2010, p. 19.

41 AFP, 'National Canine Capability' http://www.afp.gov.au/policing/aviation/canine-capability.aspx (accessed 10 May 2011).

42 ABC News, 'Amphetamine seizure a 'major blow' for illicit drug market', 7 March 2008, http://abc.com.au/news/stories/2008/03/07/2182754.htm (accessed 18 April 2011).

4.66 The Civil Aviation Safety Authority informed the committee that commercial aircraft require permission from CASA to enter Australia to ensure the regulation of safe aircraft. This did not apply to private aircraft.[43] Aircraft entering controlled airspace are required to file a flight plan with Airservices. In practice, this applied to most aircraft in general aviation.[44]

4.67 Airservices Australia noted that, from a civil aviation perspective, it was possible that small aircraft movement across Northern borders and internally were not monitored, due to the technology used. As Mr Dawson described:

> The trouble with what the committee is looking at with small aircraft and our ability to detect or to stop is that the surveillance that civil aviation has is different to what defence has—it is a different kettle of fish. Civil aviation surveillance is primarily based on transponders of an aircraft, which send out a signal and we pick that up. That is what we call secondary surveillance technology. If an aircraft wants to come into Australia from, say, PNG or somewhere in the north, and they turn that transponder off, do not file a flight plan and land in an airport where we do not have a facility, such as a town or something like that, I suspect we would never know about it.[45]

4.68 Customs informed the committee that light aircraft entering the country could be classified as either 'reported flights' or unreported/black flights'. Customs intervention on reported flights was determined by the identified level of risk associated with that flight.[46]

4.69 Customs also places resources into the Community Participation Program, through which Customs has established a network of contacts in coastal and remote areas. This network, which provides information in realtion to suspect or unusual activity, is partially drawn from individuals and organisations associated with aviation, including airport operators, aviation service providers and remote area property owners.[47]

4.70 In addition, Customs relies on information provided by external agencies responsible for monitoring Australian airspace. For regulated airspace, this included Airservices Australia.[48] Airservices Australia noted that its tower controllers in small

---

43 Mr Adam Anastasi, Civil Aviation Safety Authority, *Committee Hansard*, 18 February 2011, p. 19.

44 Mr Paul Dawson, Airservices Australia, *Committee Hansard*, 18 February 2011, p. 22.

45 Mr Paul Dawson, Airservices Australia, *Committee Hansard*, 18 February 2011, p. 22.

46 Customs, answer to written question on notice (received 25 May 2011).

47 Customs, answer to written question on notice (received 25 May 2011).

48 Customs, answer to written question on notice (received 25 May 2011).

and regional airfields did provide information about suspicious activity to the Australian Federal Police.[49]

4.71 Finally, Customs noted that Defence had the primary responsibility for identifying unauthorised aircraft movements.[50]

Issues in the maritime sector

4.72 The committee heard of a number of vulnerabilities that currently exist in port and maritime security arrangements. These vulnerabilities need to be addressed in order to inhibit and disrupt organised criminal activity in the maritime sector. Successfully hardening the maritime environment will complement the joint agency law enforcement response recommended in the previous chapter.

Varied security levels between ports

4.73 The committee visited port and associated facilities in most states and territories over the course of this inquiry. The most easily observable issue was the different level of security applied at each port. As a general rule, security was tighter at larger ports, which probably a natural consequence of the greater flow of goods through those ports.

4.74 The committee was informed that the Sydney and Melbourne container ports are the highest risk ports in Australia in terms of illicit drug importations. As Mr Jeff Buckpitt, Customs, explained:

> ...Sydney and Melbourne are the key ports of highest risk in terms of drugs entering by sea cargo. All ports are a risk, but historically if you look at where the detections have occurred the vast majority of them has been in Sydney followed then by the ports of Melbourne and Brisbane.[51]

4.75 The ACC informed the committee that the higher level of criminality assessed to exist at the major Sydney and Melbourne container ports reflected the range of vulnerabilities presented by large cargo volume, workforce size, the local criminal environment and the proximity of these ports to the major illicit commodity markets.[52] These observations support a view that organised criminal networks are likely to continue to target the major container terminals.

4.76 However, the committee is concerned that Australia's overall effort to resist the importation of harmful, illicit drugs may suffer from a 'weakest link' effect as a result of the disparate approach to port security. For this reason, the committee is keen

---

49 Mr Michael Miller, Airservices Australia, *Committee Hansard*, 18 February 2011, p. 22.

50 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

51 Mr Jeff Buckpitt, Customs, *Committee Hansard*, 17 February 2011, p. 5.

52 ACC, *Submission 8*, p. 7.

to see a harmonised approach to port security, including upgraded minimum standards in a number of areas canvassed below.

Access to the port precinct

4.77 The main area of difference that the committee observed during inspection visits was the security of port access points. Major ports had manned gates who verified the identity of incoming individuals, including checking for an MSIC. However, some smaller ports simply required a valid swipe card, with no assessment of whether the card, often integrated with an MSIC, belonged to the individual using it.

4.78 The difference in access security was observed by a number of witnesses, including Mr Dean Summers, MUA, who stated:

> But if the first question was about whether the gates, locks and guard security consistent right around the coast in every single port in Australia my answer is that I do not think it is. I think there is consideration given to large container terminals—to support your case that that is where the majority of illicit goods including drugs may come through. These are only my observations.[53]

4.79 The committee was particularly impressed with the solution adopted by the Fremantle Inner Harbour. Gates into the port security area included a video camera that enabled security guards in a central security office to verify the identity of the cardholder.

4.80 The committee is of the view that all seaports around Australia that feature a port security zone as required by MTOFSA should establish perimeter gates with facial recognition capability, either though a human operator, link to a human operator via Closed Circuit Television (CCTV) or a software-based solution.

Recommendation 10

4.81 The committee recommends that access to port security areas prescribed under the *Maritime Transport and Offshore Facilities Security Act 2003* should require verification that the Maritime Security Identification Card belongs to the individual seeking access, either through human gate operators, verification by Closed Circuit Television or any other appropriate solution.

4.82 In the next chapter, the committee recommends the incorporation of biometric information into the ASIC and MSIC, which may present opportunities for more sophisticated access control in the future.

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

Container inspection

4.83 The inspection of incoming shipping containers, through x-ray screening and physical examination, is an important deterrent against the importation of illicit goods. However, the sheer scale of containerised shipping means that the universal inspection of every container would be incredibly costly.

4.84 In 2007–08, 2.5 million containers (twenty-foot equivalent) were imported into Australia.[54] Of these, Customs inspected 138 000, and physically examined 15 500.[55] In other words, in 2007–08, 5.6 per cent of containers were inspected, and 0.6 per cent were physically examined. The percentage inspected or examined is therefore low relative to overall volume.

4.85 In order to increase the impact of inspection and screening, Customs selects containers through a cargo profiling system. All cargo entering and leaving Australia is required to be reported to Customs through the Integrated Cargo System (ICS). This information is used to assess against known and suspected indicators of border risk, including drug importation.[56]

4.86 Cargo profiles that are flagged through Customs' Cargo Risk Assessment (CRA) system are referred to cargo targeting officers for further analysis. In particular, cargo with a high or medium risk is referred for inspection or examination. A sample of low risk cargo is included for sampling and compliance purposes. Customs outlined a number of inspection and examination patterns that were adopted. These strategies balance the need to screen high risk cargo with the need to ensure that new risk patterns are identified and criminal networks cannot escape scrutiny through avoiding known risk profiles.[57]

4.87 The inspection and examination capability is also used in cases where law enforcement agencies have received specific intelligence. As noted by Mr Phelan, AFP:

> Customs and Border Protection have their own great intelligence system for selecting containers and so on. Sometimes things come cold, but in the vast majority of instances things are based on intelligence. We would know either specifically what was going to happen or in a more roundabout way that leads us to a picture to help target particular containers or vessels.[58]

---

54 Bureau of Infrastructure, Transport and Regional Economics, DITRDLG, Australia Maritime Activity to 2029–30, Statistical Report, p. 36

55 Customs, Annual Report 2007–08, p. 38.

56 Customs, *Submission 13*, p. 13.

57 Customs, *Submission 13*, p. 14.

58 Mr Michael Phelan, Deputy Commissioner, AFP, *Committee Hansard*, 17 February 2011, p.44.

4.88 The committee considers that the approach taken by Customs is intelligent, though higher rates of inspection and examination would be desirable in an ideal world.

The need for a confidential inspection mechanism

4.89 Though the committee does not wish to recommend higher rates of inspection and examination, the current system could benefit from improvement. In particular, the committee has identified the need for a confidential container inspection capability.

4.90 Currently, containers are taken to a Customs Container Examination Facility (CEF), typically located near the port precinct, for inspection and physical examination. Unfortunately, the act of moving a container in order to do so is generally recorded within port logistical databases. Trusted insiders or other corrupt employees may be in a position to access these databases and become aware of law enforcement interest in particular containers. Operational integrity cannot be maintained in this circumstance.

4.91 Specifically, the Integrated Cargo System (ICS) provides live information about the status of cargo. The ICS was developed by Customs as a single system for the management of imports and exports. The ICS features information provided by importers and exporters and transport and logistics service providers. In addition, it provides Customs and other government agency authority for cargo movement and clearance.[59]

4.92 The committee understands through its inspection visits that the ICS is accessible to an extremely wide group of people. While this meets 'emerging industry and government needs for more effective and efficient management [of] Australia's import and exports',[60] it also informs criminal elements of government interest in particular cargo.

4.93 For this reason, the committee is of the opinion that a new mechanism is required by which containers can be manipulated or taken for examination at a Container Examination Facility without alerting potential trusted insiders or criminal facilitators to the action.

---

59 Customs, 'The Integrated Cargo System (ICS) Context', http://www.cargosupport.gov.au/webdata/minisites/sdg/overview/the_ics_context.htm (accessed 20 May 2011).

60 Customs, 'The Integrated Cargo System (ICS) Context', http://www.cargosupport.gov.au/webdata/minisites/sdg/overview/the_ics_context.htm (accessed 20 May 2011).

Recommendation 11

4.94 The committee recommends the development of a system that enables the confidential movement and examination of containers that increases the likelihood that trusted insiders involved in serious or organised crime are not alerted to law enforcement agency interest in a container.

Empty containers

4.95 The committee was also alerted to the vulnerability of the empty container trade to criminal exploitation. Where the demand for containerised imports exceeds the demand for containerised exports at a particular port, the unwanted containers must be shipped to other ports empty. The Maritime Union of Australia informed the committee that this empty container trade was subject to far less scrutiny than standard container trade, with the potential for exploitation.

> With the low level of container inspections, particularly in the trans-shipment of what should be empty containers, there is no scrutiny. If a container seems light enough and is labelled as an empty container, it will come in and out, trans-shipped through different ports in the world, including Australian ports, with absolutely no visual checks.[61]

4.96 The committee was concerned by this allegation and sought more information from Customs. Customs informed the committee that all empty containers arriving in Australia are required to be reported through the ICS. Reported containers are assessed against available information to determine potential risk. Where a risk is identified, containers are referred for inspection or examination.[62] This is similar to the approach taken to loaded containers, including occasional random sampling.[63]

4.97 Export containers are not subject to the same requirements and reporting for these is limited to the number of empty containers loaded on a vessel.[64]

4.98 Customs noted that there were few contemporary examples of instances where an empty container had been identified with undeclared contents:

> Of note is that discovery has most often been associated with an additional occurrence such as a rail accident or crane failure, and not through intelligence or anomalies in reported information. The only significant find in an empty container was 640 kilograms of cannabis in June 2004. All other operations involving empty containers since 2004 have resulted in no significant finds.[65]

---

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

62 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

63 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

64 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

65 Customs, answer to written question on notice, 9 May 2011 (received 25 May 2011).

4.99 The committee notes that Customs appears to treat imported empty containers in a similar fashion to imported loaded containers. As such, they are most likely no more vulnerable than a standard container, at least from an importation perspective.

CCTV

4.100 The use of Closed Circuit Television (CCTV) is an effective tool in promoting security within both airports and seaports. The Wheeler Review, inquiring into the aviation sector in 2005, included a number of recommendations about the improvement and consolidation of cameras within the airport. The Review recommended that Customs take the lead role in monitoring the camera network, stating:

> Access control at major airports should continue to be strengthened by the reduction of unnecessary access points and enhanced monitoring. Among the Australian Customs Service's excellent capabilities is particular expertise in closed-circuit television (CCTV), and Customs should be the lead agency to improve the technology, integration, sharing and retention of CCTV data at all international airports, including associated domestic terminals, to deter and investigate crime and terrorism. Use of CCTV would be oversighted by the Airport Police Commander. Customs should also provide advice on CCTV to domestic (including regional) airports, and this will require Commonwealth legislative enablement and financing.[66]

4.101 The Wheeler Review further recommended that the CCTV system be expanded, with arrangements made to ensure CCTV standardisation, digital upgrading, storage and fully-coordinated used by Customs, police and security personnel.[67]

4.102 The committee observed during visits to major airports that Customs controls an effective CCTV network. As at November 2009, Customs maintains CCTV infrastructure at eight international airports and 63 seaports, with over 2000 CCTV cameras in all. This network of cameras links to local Customs Houses, state monitoring centres and the National Monitoring Centre in Melbourne. [68]

4.103 One important consideration is the need for all cameras to provide video footage of an evidentiary standard, to ensure that they can be used to facilitate successful prosecution following a criminal act. This was a point raised by AFPA, who stated:

> One of the issues we have raised is that the cameras need to be upgraded so they are of evidentiary value. Really, there is no point in having them there if they cannot even do that. I think a very good example was Sydney domestic airport with the outlaw motorcycle gang violence there whereby

66 Wheeler Review, p. xiii.

67 Wheeler Review, p. xix.

68 Customs, *Submission 13*, p. 12.

> they ended up having to rely on various privately owned footage and they did not cover the area where the incident happened.[69]

4.104 The maintenance of separate CCTV networks remains an issue, despite recent improvement. The committee is of the opinion that Customs should continue its lead role with access to CCTV networks maintained by both private and public entities in the airport and seaport environments. As AFPA stated:

> This is because we are relying on private systems—the one that belongs to Qantas and the ones that belong to various airlines—so you are putting a mish-mash together. We are saying that if you are talking about security at airports the focus has tended to be on Customs hauls and so forth but that the CCTV program needs to be covering the whole of the airport security area.[70]

4.105 In addition to the CCTV infrastructure itself, software-based solutions can significantly augment the ability of camera network. The AFPA noted the desirability of automated number plate recognition technology at gates, stating:

> This is where we have also raised the use of automatic numberplate recognition. It is available and it is being used by nearly all state jurisdictions, who are trialling it. We would say entry points into airports and maritime ports would be significant in regard to what that data could provide to us either before, during or after a criminal or critical national security issue.[71]

4.106 CrimTrac made a similar point, noting it could be used for both preventative and investigative purposes. Mr Douglas Smith, CrimTrac, explained:

> The purpose is twofold: to ensure that we know who has come in and out of the secure areas airside of the airport or at the port and, also, by extension it creates a capability that can be preventative and investigative. You have the ability to automatically record what vehicles have come in and that then gives you the possibility of having alerts for flagging at-risk vehicles or vehicles of interest.[72]

4.107 Finally, CCTV is relatively inexpensive compared to other security infrastructure projects. The AFPA provide some cost estimates, stating:

> CCTV is not very expensive in its total cost. It was estimated that $20 million would be the cost of upgrading airport CCTV systems across the 11 designated airports, and the estimated costing is $4 million to upgrade CCTV systems at two designated maritime general cargo ports. So, when

---

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. 34.

71 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 34.

72 Mr Douglas Smith, CrimTrac, *Committee Hansard*, 18 February 2011, p. 47.

> you look at value for money, this is a relatively low capital outlay for a significant result.[73]

4.108 The committee is therefore of the opinion that CCTV should remain a major part of the security effort at airports and seaports. The effectiveness of the network is best served through a Customs-led coordinated approach, with the potential use of imaging software.

Recommendation 12

4.109 The committee recommends that the Commonwealth government further invest in CCTV at airports and ports, with consideration of a number of ongoing improvements, including:

- **that CCTV cameras should be capable of producing footage of evidential quality;**
- **the continuing lead role of Customs in coordinating the monitoring of CCTV networks; and**
- **that CCTV networks should be complemented with automated number plate recognition, and/or facial recognition technology.**

Licensing of Customs Brokers, Depots and Warehouse Operators

4.110 Certain functions within the international import/export sector require the operator to hold a specific license under the *Customs Act 1901* (Customs Act). These include Customs Brokers and the operators of Depots and Warehouses.

Broker's License

4.111 Customs brokers play a key role in the maritime trade, with the potential for significant influence within the port environment. Customs provided information to the committee about the requirements to become a qualified customs broker. As Mrs Marion Grant explained:

> To become a qualified customs broker there is a tertiary qualification, so study to be undertaken, examinations and assessment and if successful in passing that particular qualification then they may make application for a customs brokers licence. Within our legislation we then apply an improper person check to the applicant for a brokers licence which includes a criminal record check and a financial background check. Obviously, if those checks are not successful we would not issue the brokers licence. In cases where we have already issued licences and then some noncompliance with our requirements is identified, we can do everything from sanctioning or reprimanding the broker right through to suspending the brokers licence,

73 Mr Jonathan Hunt-Sharman, AFPA, *Committee Hansard*, 17 February 2011, p. 36.

cancelling it or not renewing it depending on the severity of the noncompliance with the requirements.[74]

4.112 The committee understands that in conducting a 'person of integrity' check 'as part of the application process, Customs may have regard to:

- any conviction of the person for an offence under the Customs Act committed within the 10 years immediately preceding the making of the application;
- any conviction of an offence of any other Commonwealth, state or territory law, punishable by imprisonment of one year or longer; being an offence committed within the 10 years immediately preceding the making of the application;
- whether the person is an undischarged bankrupt;
- any misleading statements made in the application by or about the person; and
- where the statement by the person was false, whether the person knew it to be false.[75]

Depot License

4.113 A depot, under the Customs Act, is a place used for the packing, holding or unpacking of exported or imported goods.[76] The requirements for the granting of a depot license to an individual include a 'fit and proper person' test which is substantially similar to the 'person of integrity' test applied to brokers.

Warehouse License

4.114 Goods can be warehoused, meaning they are held at a warehouse either without payment of any duties and taxes until the goods are entered for home consumption or until they are exported. Operators of such a warehouse must be licensed and are responsible for the safe custody and accounting of these goods.[77]

4.115 Warehouse license applicants are also subject to a 'fit and proper person' test similar to those above.

4.116 The committee notes that none of these license requirements currently allow Customs to have regard to a person's known criminal associations or any other form of criminal intelligence. As will be discussed in the context of Aviation and Maritime Security Cards, this may leave the sector vulnerable to exploitation by trusted insiders and other criminal infiltration.

---

74 Mrs Marion Grant, Deputy CEO, Customs, *Committee Hansard*, 17 February 2011, p. 5.

75 Customs Act 1901, ss. 183CC(4).

76 Customs Act 1901, ss. 77G(1).

77 Customs, 'Warehouse & Depot', http://www.customs.gov.au/site/page6091.asp (accessed 20 May 2011).

4.117 The following chapter includes a possible model whereby a suitable law enforcement agency could make a determination that an ASIC or MSIC should be revoked on the basis of compelling criminal intelligence.

4.118 The committee recommends that a similar provision should apply in the case of licenses granted under the Customs Act. In this case, Customs would be given the power to revoke a broker's, warehouse or depot license based on its own determination that an individual or individuals were involved or strongly associated with significant criminal activity on the basis of compelling criminal intelligence. The determination could have regard to intelligence collected by Customs itself, and that provided by other law enforcement agencies.

Recommendation 13

4.119 The committee recommends that Customs be given the power to revoke a depot, warehouse or broker's license if it determines, on the strength of compelling criminal intelligence, that an individual or individuals are involved or strongly associated with significant criminal activity.

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

Appendix 1

List of Submissions

1	Mr Gregory Howarth
2	Captain Gordon Ramsay
3	Western Australia Police
4	Airservices Australia
5	Qantas Airways Limited
6	Australian Commission for Law Enforcement Integrity
7	Australian Services Union
8	Australian Crime Commission
9	Sydney Airport Corporation Limited
10	Chief Commissioner Simon Overland APM
11	Australian Transaction Reports and Analysis Centre
12	Department of Immigration and Citizenship
13	Australian Customs and Border Protection Service
14	Attorney-General's Department
15	Maritime Union of Australia
16	Australian Workers Union
17	CrimTrac
18	Department of Infrastructure, Transport, Regional Development
19	Australian Federal Police
20	Macedon Ranges Shire Council
21	Transport Workers Union of Australia
22	Confidential
23	Confidential

24 Confidential

25 Australian Federal Police Association

26 Australian Airports Association

27 Confidential

28 Confidential

29 Mr Malcolm Park

Appendix 2

Public Hearings and Witnesses

Wednesday, 17 February 2010 – Melbourne VIC

Australian Airports Association

Mr John McArdle, Chairman (via teleconference)

Australian Services Union

Ms Linda White, Assistant National Secretary
Mr Zoe Edwards, Research and Industrial Officer
Mr Stephen McInerney, Member

Thursday, 18 February 2010 – Sydney NSW

Mr Michael Carmody, Private capacity

Sydney Airports Corporation Ltd

Mr Rodney Gilmour, General Manager, Corporate Affairs, Planning and Human Resources
Mr Grant Woods, General Manager, Airport Operations

AUSTRAC

Mr John Schmidt, Chief Executive Officer
Mr John Visser, Acting Executive General Manager, Intelligence
Ms Amanda Wood, General Manger, Supervision

Ports Australia

Mr David Anderson, Chief Executive Officer
Ms Susan Fryda-Blackwell, Executive Officer

Transport Workers Union

Mr Anthony Sheldon, Federal Secretary
Mr Scott Connolly, National Executive Officer
Mr George Oei, Member

Wednesday, 10 November 2010 – Fremantle WA

Western Australian Police

Detective Superintendent Charles Carver, Serious and Organised Crime Branch
Mr Mark Padget, Leading Intelligence Analyst, State Intelligence Division

Ms Maggie Plumb, Private capacity

Thursday, 17 February 2011 – Canberra ACT

Australian Customs and Border Protection Service

Mrs Marion Grant, Deputy Chief Executive Officer, Border Enforcement
Mr Jeff Buckpitt, National Director, Intelligence and Targeting Division
Ms Roxanne Kelley, National Director, Enforcement and Investigations Division
Mr Terry Wall, National Manager, Passenger Operations
Dr Ben Evans, National Director, Law Enforcement Strategy Division

Australian Crime Commission

Ms Karen Harfield, Acting Chief Executive Officer
Mr Michael Outram, Executive Director, Serious and Organised Crime
Mrs Kathleen Florian, Brisbane Office Manager

Mr Richard Janeczko, Private capacity

Attorney-General's Department

Mr Geoff McDonald, First Assistant Secretary, National Security Law and Policy Division
Ms Tamsyn Harvey, Assistant Secretary, AusCheck

Australian Federal Police Association

Mr Jonathan Hunt-Sharman, President
Mr Ian Bridle, Vice President, Federal Operations
Federal Agent Ben Santamaria, Zone Coordinator, Federal Investigations and Office Operations Support

Australian Federal Police

Mr Michael Phelan, Deputy Commissioner, Close Operations Support
Mr Kevin Zuccato, Acting Deputy Commissioner, Operations

Friday, 18 February 2011 – Canberra ACT

Maritime Union of Australia

Mr Dean Summers, International Transport Workers Federation Coordinator

Civil Aviation Safety Authority

Mr Adam Anastasi, Acting Chief Legal Officer
Mr Peter Cromarty, Executive Manager, Airspace and Aerodrome Regulation Division
Mr Roger Crosthwaite, Manager, Permission Application Centre
Mr Peter Fereday, Executive Manager, Industry Permissions

Airservices Australia

Mr Paul Dawson, Government and International Relations
Mr Michael Miller, Manager, Security and Resilience

Qantas Airways Ltd

Mr Stephen Jackson, Head of Security and Facilitation
Mr Luke Bramah, Security Assurance and Advisory

Department of Infrastructure and Transport

Mr Andrew Wilson, Deputy Secretary
Mr Paul Retter, Executive Director, Office of Transport Security
Mr Steve Dreezer, General Manager, Maritime, Identity and Surface Security Branch, Office of Transport Security
Mr Peter Robertson, General Manager, Aviation Security Branch, Office of Transport Security
Mr George Brenan, General Manager, Transport Security Operations, Office of Transport Security

CrimTrac

Mr Douglas Smith, Chief Executive Officer
Ms Theresa van Gessel, Manager, Policy and Legal
Ms Roberta Kennett, National Manager, Background Checking Services
Mr Jeremy Johnson, Business Manager, Biometrics

Chameleon Associates (Australia) Pty Ltd

Mr Kim Langton, Managing Partner, Australia Pacific Region

Appendix 3

Site visits and inspections

Inspections of Brisbane Airport and Port of Brisbane, 30 March 2010

Inspections of Townsville Port and Airport, 31 March 2010

Inspection of Port of Melbourne precinct, 9 April 201

Inspection of Port of Darwin and Darwin International Airport, 5 May 2010

Inspection of Fremantle Port, Perth Airport and Jandakot Airport, 10 November 2010

Inspection of Port Adelaide and Adelaide Airport, 14 February 2011

Appendix 4: International and Domestic Illicit Drug Prices

(All Costs in $US)	UNODC World Drug Report 2010 (2007–08 dated figures)						IDDR 2008–09
	Source Country		United States average wholesale	United Kingdom average wholesale	Canadian average wholesale	Australian average wholesale	Australian average wholesale (recent)
	Country	Average wholesale					
Cocaine (per kg)	Colombia	$2,348 (T) (No range reported)	(No typical price reported) $10,000 – $43,000 (R)	$64,682 (T) $40,657 – $70,226 (R)	$38,761 (T) $18,025 – $64,510 (R)	$146,539 (T) $113,044 – $167,473 (R)	$150,000 – $250,000
	Peru	$1,250 (T) $950 – $1,250 (R)					
Heroin (per kg)	Afghanistan	$2,405 (T) $2,256 – $2,554 (R)	$71,200 (T) $40,000 – $100,000 (R)	$29,569 (T) $18,480 – $35,113 (R)	$119,431 (T) $75,894 – $213,452 (R)	$221,304 (T) $191,398 – $251,210 (R)	$160,000 – $210,000 (price per 700g*)
Methylamphetamine (per kg) **	Canada	$16,687 (T) $14,230 – $23,717 (R)	(No typical price reported) $3,120 – $70,200 (R)	Unreported		$120,394 (T) $75,377 – $167,504 (R)	$90,000 – $210,000
Ecstasy (per 1000 tablets)	The Netherlands	$4,111 (T) $3,426 – $4,796 (R)	$10,000 (T) $5,000 – $13,000 (R) (Data from 2004)	$6,468 (T) $4,620 – $8,316 (R)	$3,947 (T) $1,708 – $6,641 (R)	(No typical price reported) $5,914 – $25,344 (R)	$5,750 – $20,000

(T) = Typical price (R) = Price range

Note: This table is based on drug prices sourced from the UNODC *World Drug Report 2010*, which uses data from 2007–08, this being the most contemporary and reliable international data source available at this time. In addition, 2008–09 wholesale prices, sourced from the ACC's *Illicit Drug Data Report 2008–09*, are provided as an indication of price changes domestically between 2007–08 and 2008–09.
Prices do not take into consideration purity. Prices are indicative only, as they may vary both within and between countries.

* Australian law enforcement agencies did not report prices per kilogram. Prices per 'Asian catti' (700 grams) were the closest available data set.
** Prices may be influenced by form (eg: powder or crystal). Note that the majority of methylamphetamine consumed in Australia is domestically produced.